Fuzzy logic and its application to dynamic security assessment of electrical power systems

Groom, C. G.

Award date:
1994

Awarding institution:
University of Bath

FUZZY LOGIC AND ITS APPLICATION TO DYNAMIC SECURITY ASSESSMENT OF ELECTRICAL POWER SYSTEMS

Submitted by C. G. Groom, B.Eng.(Hons)
for the degree of
Doctor of Philosophy
of the University of Bath
1994

C. Groom

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

Summary

A new artificial intelligence based approach for security assessment of an electrical power system is presented in this thesis. A single processor version of the multi-machine power system simulator, developed at the University of Bath, has been used as the basis of this research. Traditional techniques for contingency analysis, evaluation and system stability assessment are discussed, together with applications of artificial intelligence in these areas.

The concept of fuzzy set theory is described and the development of algorithms for contingency evaluation and stability analysis is discussed. A demonstration is shown, illustrating how such a method could be used to assess the security/stability of a number of test networks. These range from 6 network nodes and 4 generating groups to 718 nodes and 93 machines. Results are presented for these fuzzy methods, with different weighting functions, and compared with two numerical approaches. The latter consist of the more traditional techniques for contingency analysis and include one which is known to be free from errors, which is used as a benchmark for the other methods. Time domain solutions are used to verify the stability assessment made by the new fuzzy approaches.

Conclusions are drawn in the light of these results, discussing the effectiveness of the fuzzy techniques with respect to computational speed advantages that can be obtained and without loss of accuracy when compared to the benchmark. Future developments of the basis simulator and the assessor algorithms are also suggested.

Acknowledgements

The author would like to thank Mr. A. R. Daniels, Project Supervisor, and Dr. R. W. Dunn for their continued support and encouragement throughout the course of this research.

I would also like to thank Professor A. T. Johns, Head of School, for the provision of facilities at the School of Electronic and Electrical Engineering and Mr. V. S. Gott and Mr. B. Ross for providing excellent technical support.

Grateful thanks are extended to the staff of National Grid Company plc, particularly Mr. P. H. Buxton, Industrial Supervisor, and Dr. M. E. Bradley for their support, technical discussions and supply of information. Additionally, I would like to acknowledge Dr. I. A. Erinmez, Mr. M. J. Rawlins, Dr. N. H. Dandachi and Dr. A. O. Ekwue for their contributions throughout this research. The efforts of Mr. T. J. Harrison are gratefully recognised for dealing with financial and placement problems.

Finally I would like to thank Dr. K. W. Chan for some interesting technical arguements and Mr. J. M. Grzejewski, Mr. A. R. Edwards and Mr. K. R. W. Bell for an enlightening working atmosphere.

This work was carried out under a SERC[1] CASE[2] award supported by the National Grid Company plc.

This thesis was prepared using LaTeX with PiCTeX for graph plotting.

[1]Science and Engineering Research Council

[2]Co-operative Award in Science and Engineering

Contents

List of principal symbols

General

h integration timestep
p differential operator, $\frac{d}{dt}$
j complex operator
t time in sec

Synchronous Machine Equations

Variables

I_d direct axis current
I_q quadrature axis current
V_d direct axis component of terminal voltage
V_q quadrature axis component of terminal voltage
V_t terminal voltage magnitude
V_f field voltage referred to stator terminals
E'_d direct axis voltage behind transient reactance
E'_q quadrature axis voltage behind transient reactance
E''_d direct axis voltage behind sub-transient reactance
E''_q quadrature axis voltage behind sub-transient reactance
S_d direct axis magnetic saturation factor
S_q quadrature axis magnetic saturation factor
T_a accelerating torque
T_e electrical (air gap) torque
T_m mechanical torque
T_{mo} mechanical torque constant
T_{lo} mechanical loss torque
K_e machine kinetic energy in kg rad/sec^2
A_{cc} machine rotor acceleration in rad/sec^2
δ machine rotor angle in rad
ω machine angular velocity in rad/sec
ν normalised angular velocity
s slip

Parameters

X_d direct axis reactance
X_q quadrature axis reactance
X'_d direct axis transient reactance
X'_q quadrature axis transient reactance
X''_d direct axis sub-transient reactance
X''_q quadrature axis sub-transient reactance
R_a winding resistance
n generator transformer tap ratio
R_t generator transformer resistance
X_t generator transformer reactance
Y_{re} real part of machine admittance
Y''_d direct axis component of sub-transient reactive admittance
Y''_q quadrature axis component of sub-transient reactive admittance
T'_{do} direct axis open circuit transient time constant
T'_d direct axis transient time constant
T'_{qo} quadrature axis open circuit transient time constant
T'_q quadrature axis transient time constant
T''_{do} direct axis open circuit sub-transient time constant
T''_d direct axis sub-transient time constant
T''_{qo} quadrature axis open circuit sub-transient time constant
T''_q quadrature axis sub-transient time constant
H inertia constant in MWsec/MVA
M $H/(\pi f_0)$
ω_0 rated frequency in rad/sec
f_0 rated frequency in Hz

Control System Models

AVR variables

V_r regulator reference voltage
V_{err} error voltage
V_a regulator output voltage
V_s excitation stabilising voltage

AVR parameters

K_g forward path gain (simplified model)
K_a regulator amplifier gain
K_e exciter constant related to self-excited field
K_s regulator stabilising circuit gain
T_g forward path time constant (simplified model)
T_a regulator amplifier time constant
T_e exciter time constant
T_s regulator stabilising time constant
T_d regulator stabilising damper time constant
S_e exciter saturation

Governor variables

V_{dem} steam control demanded valve position (simplified model)
V_{vpos} steam control actual valve position (simplified model)
T_{m1} high pressure cylinder torque
T_{m2} low pressure cylinder torque
W_g governor speed reference
W_i interceptor speed reference
V_{pg} steam control valve position
V_{pi} interceptor valve position
P_{gv} power at control valve outlet
P_{iv} power at interceptor valve outlet
P_b boiler power
P_c high pressure turbine power
P_r low pressure turbine power
P_m mechanical power

Governor parameters

K_t feedback gain (simplified model)
T_a first lag stage time constant (simplified model)
T_b second lag stage time constant (simplified model)
T_c third lag stage (reheat) time constant (simplified model)
K_1 proportion of power from high pressure cylinder (simplified model)

continued on next page

continued from previous next page

K_g governor controlled gain
T_g governor controlled valve time constant
T_i interceptor valve time constant
T_c steam chest time constant
T_r reheat time constant
R_g regulation of speed governor loop
R_i regulation of interceptor loop
K_h high pressure turbine power fraction
K_l low pressure turbine power fraction
K_i interceptor valve gain

Network Equations

E machine internal voltages
$\boldsymbol{I}$ vector of current injections
$\boldsymbol{V}$ vector of busbar voltages
$\boldsymbol{Y}$ nodal admittance matrix

Network element

r_l resistance
x_l reactance
b_l susceptance

Fuzzy Sets

General

A fuzzy subset
U universal discourse
μ membership function
x variable in subset A

Operations

$\neg A$	Complement of A
$A + B$	Union of A and B
$A \times B$	Cartesian product of A and B
$A \cup B$	Intersection of A and B.
AB	Product of A and B
$CON(A)$	Concentration of A
$DIL(A)$	Dilation of A
$INT(A)$	Contrast Intensification of A

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Electrical Power System Operation

Since the industrial revolution, the demand for and consumption of electrical energy has steadily increased. Very complex power systems with an interconnected network of transmission lines linking generators to loads have been built in all the worldwide developed countries, in order to meet this demand.

Successful operation of such a power system presents many engineering problems which provide the engineer with a variety of challenges. These demands include planning, construction and operation of such systems and, in order to predict the performance of a typical power network, the engineer is forced to rely on ever more powerful tools of analysis and synthesis.

The basic objective of an electrical power system is to supply energy to the various loads distributed throughout the network [1]. Properly designed and operated, it should, therefore, meet the following requirements : -

- It must supply energy to every customer demanding it.
- It must be able to cope with time varying load demands for real (MW) and

reactive (MVAr) power.

- The "quality" of supply to these loads must meet certain utility specific constraints, in terms of frequency, voltage and high reliability.
- It should deliver energy at the lowest economical and ecological costs.

The control of synchronous generators to maintain their parallel operation with sufficient capacity to meet load demand is one of the primary objectives for a reliable service [2]. The system frequency serves as an indication of any unbalance between consumed and generated power and can be used to control the power output of the generator via its governing system. If at any time a generator loses synchronism with the rest of the system, significant voltage and current fluctuations may occur and transmission lines may be automatically tripped by their relays. This is, therefore, a potential *stability* problem. If a generator is separated from the system, it must be resynchronised and then loaded without detrimental effect to either the rest of the connected network or to the customer.

The second primary objective for a reliable electricity supply is to maintain the connectivity of the power network. The high-voltage transmission system connects the generating stations and load centres. Interruptions to this network will ultimately hamper the flow of power to the load. Also, in attempting to transmit electrical energy via a transmission link, a limit will be reached, beyond which no more power can be carried by that line. This constraint introduces the concept of *static transmission capacity.* Power flows between neighbouring power systems over interconnecting tie-lines often help maintain the continuity of service of each network . Therefore, successful operation of the system relies on these lines remaining in service, if power is to be exchanged between areas of the system.

In addition to maintaining power-load balance, control of network voltage levels also needs to be addressed. An unchanged busbar voltage profile represents the balance between generated and consumed reactive power, in much the same way as frequency is used for the real power case. Whenever the magnitude of a particular busbar voltage changes, the implication is that the reactive power or Q balance has not been kept at that busbar. Local Q generation can be achieved by shunt capacitors and/or series compensators. However, automatic voltage regulators on generators or automatic load tap changing transformers are more readily used.

The management and control of power system is thus a very complex process and is normally, depending on the utility in question, split into increasing orders of "command hierarchy" on differing time scales [3]. These levels include : -

1. System planning - 6 months to 10 years.
2. System maintenance - 1 week to 6 months.
3. Unit commitment - 4 hours to 1 week.
4. Economic dispatch - 10 minutes to 4 hours.
5. Frequency and voltage control - 1 second to 10 minutes.

Stages 3 and 4 above are significant features in modern power system operation [4]. This is because a great deal of saving can be gained by minimising costs introduced by line losses, start-up, shut-down and maintenance costs. These reductions can be made by three functions : -

- Short-term forecast or load prediction, where a knowledge of industrial and

residential load demand is required (usually from historical recorded data) and a prediction of the forth-coming weather conditions.

- Unit commitment or scheduling of generators, where the objective is to have, at all times, the optimum number of generators on-line to provide the load demand and system reserve. "Spinning reserve" (standby synchronised generation) is also maintained in case of forecast errors or network disruptions due to system faults.

- Economic dispatch, which is the most economic loading of generators, once they are either committed or running on-line. In the UK, a calculated *merit order* schedule is used in order to load the cheapest generating sets first to their maximum outputs, reserving other, more expensive plant, for sudden or unexpected load increases.

One of the main concerns in the operation of a power system is its security. The ultimate goal is to continuously fulfil the load requirements, i.e. the generation-load balance mentioned above, without violating the operational constraints (i.e. to use transmission equipment within its associated permissible limits). Predominately, the reasons for these violations are usually associated with the forced outages of generators and transmission equipment.

The need for power system operational tools for grid control engineers has been continually highlighted since the early-1970's [5, 6]. Original control systems, dedicated purely to supervisory control or generation control, were found to be inadequate for the growing capacity and demands of large high-voltage interconnected transmission networks. A new "wave" of power system control systems has emerged with a much broader view of system monitoring and control with the addition of a new concept, that of *system security.*

The operation of a power system can, essentially, be broken down into three main sets of constraints, namely load, operating and security limits. The concept of the first two has already been explained and can be used to define a security constraint. Thus the security of the system is the ability or capability of the system to withstand a set of contingencies (unplanned outages, which include busbar faults, load and generator losses and transmission lines trips), without violating the load and operating constraints in the remaining system.

Hence, security assessment of the current operating condition of the network, with respect to a set of worst case contingencies, is another important function of power system operation. A study of this area can ultimately lead to aiding the operator to formulate a set of preventative and/or corrective actions.

1.2 Computing Applications

All of the operational functions, mentioned in the previous section, are carried out in one form or another by digital computers. These may be stand-alone machines, such as personal computers or work stations, or mainframe-based calculation engines linked to the Energy Management System (EMS). The introduction of the Supervisory Control and Data Acquisition (SCADA) system collecting information throughout the power network, allows the display of that data at the control centre. It can also have the ability to operate devices at remote locations from the control centre. The SCADA function, although not considered a system security device itself, is clearly one of the most important components in power system security.

For most power system operation functions a basic load flow, either d.c. or a.c., is often used. The power output of all generators (except that connected to the slack bus) are specified, together with generator MVAr limits and loads in MWs

and MVArs. The load flow program [7, 8] calculates the generator MVArs, all bus voltages (magnitudes and angles) and all line flows. It is undoubtedly the most valued and widely used program available to an operator, either at the on-line or planning stage. It is often used with telemetered data from the SCADA system to determine either the present state of the system, or in the case of security assessment, the future operating conditions during contingency analysis studies.

An optimal load or power flow solution is often used to optimise both real and reactive power generation [9]. Here the network equations are solved just as an ordinary load flow but, in addition, minimum and maximum ranges for each generator power are calculated. The optimal power flow can also be used to determine the economic allocation of generation with reference to the cost curves for each unit and, hence, performs an economic dispatch along with solving the total network. If instead of the desired generator terminal voltage, a range of terminal voltages for each unit is specified, both MWs and MVArs can be optimised in a P-Q dispatch.

The optimal power flow, with additional logic, could be used to avoid operating conditions where either line flows or voltage constraints are violated during normal operating conditions or during contingency applications. Corrective strategy logic could be incorporated to avoid line limits by, for example, shifting generation away from the economic optimum for those units. This, however, has the effect of moving the system away from its optimum operating point, and security is thus traded for economy.

With the increasing power of processors, new technologies for assessing system stability and security and simulating the power network itself are becoming of interest to the grid control engineer as an on-line operational aid.

1.3 Artificial Intelligence

As previously mentioned in an earlier section, the function of the EMS is to ensure that the power system is operated as securely and economically as possible. This is in addition to providing some form of interface between itself and the human operator to permit routine tasks to be carried out such as security analysis, optimal power flows, economic dispatch, unit commitment and load forecasting. These are all conducted in the "steady state" operating mode of the power system.

The situation, however, changes radically during disturbed conditions, since the above functions are of little use to an operator and the EMS becomes simply a data gatherer and reporting device. The quantity of information and the rate at which it is collected can often overwhelm the operator in such situations.

Modern power systems are ever increasing in complexity and are being operated closer to their limits so that generation and transmission assets are more economically utilised. This has a knock on effect on the operator, who, in turn, has to make quicker diagnoses and decisions about the system operating state. The implication is that with system complexity steadily increasing, the operator's ability to cope with its decreases [10] unless new techniques are designed to enhance this capability.

This illustrates the need for a new generation of EMS constituent programs, which can deal with the solution of "diagnostic and decision" processes. These are often based on the experience of operators (in coping with emergency conditions that can arise on the power system) with an ability to associate an existing situation with events learnt from the past (heuristics) to solve these problems. New techniques have been developed, under the "umbrella" of *Artificial Intelligence* (*AI*), which

can effectively mimic the operator. They can also provide a guidance about what the power system is actually doing and, in some cases, carry out some of the routine tasks, allowing the operator to spend more time on jobs of greater importance.

Since the early-1980's, a number of artificial intelligence techniques have been developed for solving problems in various fields of power systems including planning, operation and control [11–17]. System analysis approaches have been applied to detect different modes of instability [18–21] in recent years. On the operation side, alarm processing [22–25], fault diagnosis [26, 27], system restoration [28–31], load shedding [32], voltage and reactive power control [33–37] and security analysis in the form of contingency screening and evaluation [10, 38–42] have all been covered. Unit commitment, maintenance scheduling and load forecasting [43–48] have also been addressed by AI techniques.

In these applications, a number of AI methods have been used. These consist of rule-based expert systems, distributed and general problem solving (frame-based) methods, logic modelling and programming, object-oriented programming and a variety of search mechanisms, as well as the relatively new introduction of artificial neural networks.

Most rule-based systems are, inherently, three stage functions, i.e. a knowledge base, an inference engine and an user interface. The inference engine reads data from the knowledge base, decides whether to use it and, if so, carries out the execution. It has, in this respect, acted as an interpreter. However, traditional expert systems have dealt with what was, in effect, a complex yes-no processing mechanism. The concept of *Fuzzy Logic* [49–51] has evolved which, not only provides this facility but, also, adds an extra dimension by which a "maybe" statement could be introduced. This, therefore, allows fuzzy expert systems to

model human operator performance, since rule-bases are, inevitably, filled with imprecise data. These rules may contain useful information which would otherwise be meaningless to more traditional expert system/logic mechanisms.

With the ever increasing complexity of network operation and the growth of computer processing power, the use of AI techniques will become more dominant in the EMS functions of future power systems. However it is unlikely that they will ever replace the operator in the control room.

1.4 About this Thesis

Chapter 2 introduces the concept of power system security assessment. Contingency screening, analysis and evaluation are discussed together with procedures and application techniques that have been previously developed, based on numerical and artificial intelligence approaches.

Modes of instability, namely transient, steady state/dynamic and voltage stability are described in Chapter 3, with a discussion of the differences between each of these. Methods of detecting these modes are also described. Details of alarm processing and its approaches are examined in this chapter, highlighting the importance of such a facility as part of a security assessment algorithm.

Chapter 4 presents a type of artificial intelligence known as *fuzzy logic*. A simplistic verbal overview is given together with a more detailed mathematical insight into fuzzy set techniques. Applications to power systems and other examples are also discussed.

The real-time power system simulator PowSim, developed over a number of years

at the University of Bath, is briefly described in Chapter 5. Further enhancements made to the basic simulator code in order for a more detailed and, hence more accurate, contingency analysis to be carried out are also presented.

A number of computing hardware platforms have been used in the course of this research, namely a Microway Number Smasher-860 accelerator card based in a personal computer and a Silicon Graphics Indigo. Each architecture is described with its associated software operating system in Chapter 6.

Chapter 7 presents the software code implementation of the security assessor developed during this research, which has been integrated with the simulator PowSim. In keeping with Chapters 2 and 3, the code, written in ANSI standard C, has been split into contingency analysis, stability assessment and alarm processing.

A discussion of the results obtained from a fuzzy set and a more traditional numerical based security assessor is made in Chapter 8. A number of networks were used which include : a reduced system of the UK National Grid consisting of 20 machines and 100 busbars, a further reduction of this network to 4 machines and 6 busbars, as well as an IEEE 57-bus test system and a full NGC network.

Conclusions and suggestions for further work are discussed in Chapters 9 and 10 respectively.

Chapter 2

Security Assessment

2.1 Introduction

A definition of security is one of freedom from risk or danger. Power systems, however, can never be absolutely secure in this precise sense and the term is redefined as the ability of the power system to continue normal operation despite the occurrence of any one of a pre-selected list of credible disturbances or "contingencies", i.e. the level of risk at any time of disruption to the system's steady state operation. The whole concept of security has become increasingly of interest to power utilities and research organisations alike, since power networks are being operated ever closer to their stability limits due to cost, efficiency and environmental constraints.

Security assessment is becoming a valuable tool in the analysis of power system operation. It is, however, probably the most time-consuming function in an Energy Management System (EMS), since on-line contingency analysis is performed automatically (typically every ten to twenty minutes) and after any major network topology change, as well as on control operator request. For each contingency case, system performance and reliability are calculated from post-fault quantities that include power flows and busbar voltages.

For a large power system, hundreds or, in some cases, thousands of credible contingencies would need to be fully analysed within very short time intervals. This imposes a considerable computational burden, which is often too much for real-time applications, even if fast solution methods are used. In order to relieve the operator, a systematic approach to automatically select the critical contingencies is required, since a complete evaluation of all credible contingencies reveals very often that a large number pose no threat to the security of the power system. Such a method also ranks these contingencies in their ascending order of severity, so that full contingency analysis can be performed starting with the most severe at the top and proceeding down the list to the least severe. Theoretically, if a contingency no longer produces system violations, the analysis could be stopped, since it can be assumed that all the remaining contingencies are also violation free. This, in practice, does not always happen due to approximations and inaccuracies in the ranking, so that analysis is often continued for several cases down the list until no further limit violations are produced.

Brief overviews of security and contingency analysis will now be given, with following sections describing Automatic Contingency Selection (ACS) methods that have been developed and how this type of approach may be implemented as part of a dynamic security assessor.

2.2 Security Analysis

A complete on-line security analysis module is a composite of three basic components which are principally monitoring, assessment and control [52]. These can be tied together in the following way :

1. *Security Monitoring* : from real-time data, an analysis is conducted to ascertain whether the system is in a stable operating mode. If not, remedial actions need to be taken to bring the system back to a normal state, or in the case of loss of load, service restoration needs to be performed.

2. *Security Assessment* : if the system is operating in a stable mode, a set of contingencies is applied to determine whether the system is secure post-fault.

3. *Security Enhancement* : if the system is insecure during or after a contingency, some preventative measures need to be formulated and performed to make the system stable.

The main elements of a typical on-line security analysis program implemented by a number of power utilities is shown in Figure 2.1. Measurements via the computer-based Supervisory Control and Data Acquisition (SCADA) system are telemetered from around the network to the utility's EMS computer. There are principally three types of real-time measurements :

- Analogue, that include real and reactive power flows through transmission lines, real and reactive power injections of generation or demand at busbars and busbar voltage magnitudes.
- Logic, that consist of switch states, transformer Load Tap Changing (LTC) positions and the status of circuit breakers.
- Pseudo, that may include forecasted busbar loads and generation

Errors and noise may be contained in these measurements so that these are rejected by passing the newly acquired system data through a filter of reasonability

and consistency checks. The filtered measures are then passed to the topology processor to determine the system configuration of generator and transmission network connections.

The remaining data is processed still further by observability analysis of the network. This needs to be conducted before state estimation is executed, in order to determine whether enough of the system is observable for state estimation to be performed. If the set of measurements is sufficiently large with a wide distribution across the system, the network is deemed to be observable. Unobservability can occur when there are unplanned topology changes or telemetering failures.

The state estimation program is a mathematical procedure used for calculating the "best" estimate of the remaining unknown state variables of the power system based on the available data, i.e. values that can neither be measured or have not been measured. These estimates are, however, generally corrupted with errors due to delay or noise effects either in data transmission or in the communication system respectively. The state estimation process itself may introduce further errors from approximate network model parameters such as line impedances (which are impossible to measure practically) or state estimation measurements.

The best estimate of the system state is formulated as a weighted least square error problem, which is assumed to be small.[11] Occasionally, large errors or corrupted data occur and it is important to include an extra feature, as part of the state estimation program, to detect the presence of these, identify which measurements are bad and to remove all the bad data before it corrupts the results of the state estimation algorithm.

To assess whether the system is operating in a stable mode, a set of contingencies is needed. For a large power system, the number of possible contingencies is enormous and, hence, a selection process is required to reduce this list to a handful of important disturbances. To assess the system response to this reduced set, an evaluation is carried out using on-line ac load flows. This uses the state estimated solution network and an external network model, i.e. the unmonitored system of a neighbouring network, since the response of the external system also needs to be included. A bus load forecast is also implemented since the concept of a contingency is something that is a future event.

State estimation and, hence, observability analysis and bad data processing have not been included as part of this research. The main thrust is in the area of contingency analysis, so this will now be described in more detail.

2.3 Contingency Analysis

Most power utilities use two main methods for operational security assessment [38]. These are namely off-line studies, which are predominantly used at the planning stage and give advice for periods of about a day and, on-line studies, which are used at the operational stage and give guidance for periods of tens of minutes. Both methods use a similar algorithm and perform essentially the same steps : -

1. Select a base case.
2. Select a set of contingencies
3. Evaluate these contingencies
4. Display the simulation results for system operators.

For on-line contingency analysis, the current operating state of the power system is used for the base case in step 1, where data is collected automatically from the EMS. In the case of off-line studies, the base case is collated from historical data and more up-to-date EMS data is prepared for it.

The contingency set in step 2 is a list of unplanned outages of one or more power system components, such as transmission lines, transformers or generators. This list is initially chosen off-line by a human expert but amendments to the original set may be entered by an operator at the on-line stage to deal with specific conditions under which the system may be presently operating. The length of contingency lists has grown considerably with time, so that full evaluation of the entire set proves practically impossible for most EMS computers to cope with. This growth is mainly due to the necessity to include contingencies which deal with all possible power system operating conditions, which, for the majority of cases, do not adversely affect the operating states. Because of this, the most recent area of development is that of automatic contingency selection which will be described in more detail in the next section.

Contingencies that have been selected for further analysis are evaluated in step 3 by a full ac load flow. Numerical results from each evaluation are screened to detect limit violations and are presented to power system operators. Because of the increased length of contingency lists, a corresponding growth in output results has meant that for on-line security assessors this data is limited by listing only the worst violations. These are usually in terms of percentage limit violations (often referred to as alarms) for each evaluated contingency and the mechanism by which this reduction is conducted is known as "alarm processing" which will be described in greater detail in the next chapter.

To further reduce the information presented to the operator, severity indices, calculated by contingency ranking methods, have been used but this has the disadvantage that not enough specific information about the nature of the problem is presented and there is no provision of a basis from which corrective actions may be formulated.

2.4 Automatic Contingency Selection

Many automatic contingency selection methods have been developed which rely on the use of a system-wide performance index (PI) to quantify the severity of each case in the contingency list. This PI is often subsequently used for contingency ranking which is, itself, heavily dependent on the form of the PI selected. The general structure of such an index is :

$$PI = \sum_{i=1}^{N} w_i \left[f_i(x)\right]^n \tag{2.1}$$

where $f_i(x)$ is a linear function of x_i which denotes either (P_i/P_i^{max}), $(\Delta V_i/\Delta V_i^{max})$ or $(\Delta Q_i/\Delta Q_i^{max})$, the MVA transmission line flows, changes in load busbar voltage magnitudes or generator busbar injections with respect to their corresponding ratings. w_i is a real non-negative weighting coefficient and the differences between the PI's is dependent on the choice of this number. In general, the value of this coefficient is chosen so that severely violated contingencies have a performance index greater than those that are lightly violated. The PI is calculated for all the lines and/or busbars in the network and summed to yield the total system severity index (SI).

Most of the recent developments use an algorithmic approach based on a quad-

ratic function of the perfomance index, i.e. the exponent $n = 2$. This makes contingency ranking prone to masking effects, i.e. a contingency with many small limit violations can be ranked equally with one with a few large limit violations. Methods described by Halpin et al. [53] and Schäfer et al. [54] whereby the weighting coefficient w_i and the exponent n are maximised to increase the "capture rate[1]" of critical contingencies produce a reduction in masking errors in the final contingency ranking. There is, however, a corresponding increase in CPU time, so that a trade-off between accuracy and speed of execution has to be made.

2.4.1 Past Developments of ACS Algorithms

Wollenberg et al. [55] were, in essence, the first researchers to recognise the problems of evaluating large contingency lists and produced a selection algorithm to reduce the initial set to be applied for full ac analysis. A gradient method was developed to describe the system wide performance index to quantify real power circuit overloads and abnormal system voltages using a PI of the form in Equation 2.1. First order derivatives of these indices with respect to system parameter changes were calculated from Tellegen's theorem and then used to rank each contingency.

The general functional block diagram, as developed by Wollenberg in [55] is shown in Figure 2.2 and is still the basis for more modern automatic contingency selection algorithms. Performance indices are calculated for each contingency from Equation 2.1 and ranked by ordering the greatest severity at the top of the list to the least at the bottom. A fast decoupled load flow (FDLF) is carried out to give

[1]The Capture Rate (CR) is defined as the fraction of the worst N contingencies appearing in the first N entries in the ranking list. With CR < 1, the ranking will not contain the N worst contingencies.

busbar voltage or circuit overload problems for each post-contingent system state. A full ac load flow still needs to be conducted but only for those cases that produce limit violations. The stopping criteria is such that if no problems are indicated, the full analysis load flow is terminated. Ranking of those contingencies below the stopping point is still preserved, since non-limit violating cases have already been ranked. Wollenberg suggested that this was an "adaptive contingency processor" since the number of cases to be solved would vary with system conditions.

The concept of "effectiveness profiles" was also introduced [55], which was essentially a graphical representation of the performance index calculated from a dc load flow versus contingencies ranked by the algorithm. From the results described, various "bumps" were shown to be present in the profile of this graph, which was the influence of misrankings by the masking effect, although this was not known at the time.

This method was improved by Wollenberg et al. [56] by including all terms of the Taylor expansion series for changes in performance indices. The notion of masking was introduced, caused by the exponent n in Equation 2.1. Wollenberg discovered that by setting the weighting coefficient w_i in the new ranking algorithm [56] to zero, the effects of masking could be greatly reduced. A new effectiveness profile was displayed in the results which showed a much smoother decreasing slope.

Using [55] as the basis of their research, Irisarri at al. [57] used dc load flows to calculate performance indices for quantifying line overloads. A normalised function of the angle across the line was introduced rather than the MW flow which had been used previously. Both types of performance indices were tested on real-time conditions using an American Electric Power Corporation (AEP) network. The behaviour of the new PI was found to be better at non-misclassifications of line

contingencies than that in [55]. The method was further developed to include second order effects using elementary differential calculus. Although the results of this extended method were better than those obtained from the first order approach, the improvement was not vastly significant. Irisarri concluded that a dc load flow provided a competitive alternative to ACS methods and that for on-line contingency analysis, the possible use of this solution method should be considered for selection of serious line contingencies.

In a follow-up to this initial research, Irisarri et al. [58] described an efficient computational procedure for the implementation of a dc load flow involving a forward-backward substitution mechanism in order to reduce its computational demands. Further tests using the AEP system were conducted for this modification to measure the accuracy of results and concluded that the new method was at a level comparable to those of the sensitivity methods in [57]. The problem of masking was also addressed and although attempts were made to eliminate the exponent n (i.e setting it to 1) to solve some of the problems, Irisarri concluded that to remove masking errors, a number of different performance indices should be used.

To address voltage problem contingencies, which had been ignored by previous research activities, Albuyeh et al. [59] examined the automatic contingency selection of those cases causing unacceptable voltage profiles using the first iteration of a full ac load flow, since dc load flows do not indicate voltage violations. Outages were ranked using performance indices describing both real and reactive power equations, based on their calculated severity. The capture ratios were equivalent to those from a full ac load flow but, it was noted that ranking by real and reactive power PI's should be conducted independent of each other.

Sackett et al. [60] introduced a contingency analysis program that calculated changes in linearised post-contingent real power flow. Using the relationship described in [60][2], a speed-up was identified by calculating the "explicit inverse" (triangular portion) of H by a back substitution method. It was shown that multiple outage contingencies required effectively the same time as the same number computed individually.

Vemuri et al. [61] presented a unified approach to calculating the sensitivity of the PI for single outages, generation/load outages or a combination of both and concluded that, although this new method was less accurate than that of the dc load flow, it was faster with better storage requirements, making it more applicable to on-line requirements. As part of an overall ACS algorithm, Vemuri concluded that the inclusion of secondary outages was necessary and the complexity of computation was similar to that for single outages.

The identification and ranking of credible outages in dependent variable space was carried out in an algorithm developed by Wasley et al. [62]. Simple computational procedures using a single iteration of an approximate load flow were applied for each contingency case.

Lauby et al. [63] compared three methods of contingency selection of line outages causing voltage problems. A performance index and full ac load flow were used which, although performed well in detecting widespread severe volt problems, it was not suited for local area deviations within the network. Hence a local solution method (based on concentric relaxation and Gauss-Seidel solution techniques) was introduced which performed faster and better than a single iteration of a decoupled

[2] $\Delta P = H\Delta\theta$, where ΔP is an n vector describing real power changes, $\Delta\theta$ is an n vector of busbar angles and H is an n by n matrix relating ΔP and $\Delta\theta$

load flow. This approach also highlighted contingency cases which were overlooked by the linear load flow method.

A method used for improving the efficiency of ACS algorithms was developed by Halpin et al. [53], by maximising the capture rate, whilst minimising the "false alarm rate[3]" and hence masking effect without increasing the computational demand. An algorithm for calculating the weighting coefficients of the ranking PI was developed and a distinction was made between the use of performance indices and the screening approach of the fast decoupled load flow method. It was concluded that this PI method with its adaptively altered weighting coefficients could match the accuracy of the more conventional approach without sacrificing computation speed.

A voltage contingency selection algorithm based at AEP to assess line outages on load busbar voltage profiles was described by Irisarri et al. [64]. It was based on the real power portion of the FDLF to evaluate post-contingent angles and then the reactive power part of the FDLF was used to determine the post-contingent voltages. From this, a quadratic performance index for each contingency was calculated, and the PI values were sorted in descending order. Chen et al. [65] later elaborated this work and, by using a different reactive power model, a method was developed which was much faster than [64] using sparse vector and matrix techniques. From the results in the literature, approximately the same accuracy as the FDLF was obtained but with less computation time.

To compensate for the masking effect in contingency ranking, Schäfer et al. [54] introduced an adaptive procedure to improve the accuracy in PI-based techniques.

[3]The False Alarm Rate is defined as the number of false alarms or limit violations appearing in the worst N contingencies.

The process was based on the fact that on-line security analysis is carried out cyclically, so that comparisons in ranking after each outage allows updating factors to be estimated whilst taking into account a sequence of former system states. By this straight approximation of the effectiveness profile (see [55]), the procedure combines the computational speed of a quadratic PI function ($n = 2$) with the masking free but more CPU expensive PI function with $n = 20$.

Wollenberg et al. [66] developed a fast method for contingency screening and evaluation for voltage security analysis, using [64] for the basis of their research. A voltage subnetwork was determined for each contingency case within which voltage problems were highlighted. If there were no resultant violations, the contingency was deemed to be not harmful to the system state and consequently screened out. Fast forward and backward substitutions were then performed for voltage deviant cases to determine the busbar voltages within the subnetwork. For those contingencies deemed to be important, a full ac loadflow was carried out via an "adaptive reduction equivalent network" (based on concentric relaxation techniques), so that computational time was kept to a minimum.

Using this as the basis of their research, Lauby et al. [67] developed a method using an efficient bounding technique for line flow limit violations and extensions to reactive power (MVAr) mismatches at load busbars. This effectively reduced the number of consequent power flow calculations as well as the number of busbars where MVAr mismatches were to be calculated, with the main advantage that it was adaptable to any system condition or network topology. More recently Hadjsaid et al. [68] described an approach for fast contingency screening for voltage-reactive considerations in security analysis. This again was based on a bounding approach between busbars nearest to the contingency outage and those electrically distant away from the disturbance. The concept of electrical distance

was introduced in order to identify those busbars which would see the greatest voltage deviations. Hence, the number of busbars for MVAr mismatch calculations were greatly reduced and with the use of sparse vector techniques, faster computation speeds were obtained.

Ekwue and Laing [69] investigated methods for improving the accuracy and reliability of a technique which used a second order load flow method based on rectangular coordinates and the performance index in [62]. This used the load curtailment needed to raise busbar voltages to the pre-contingent level as an indication of the severity of the contingency. This is a continuation of the earlier work by Ekwue [70] based on a decoupled technique for voltage drop and line overloads using a second order load flow and misranking compensation for single line evaluation. Ekwue also investigated PI's [71] for contingency ranking of generator reactive power violations as well as real power line flow problems.

A contingency selection algorithm for dynamic stability studies was developed by Hsu et al. [72] which used the results from the first iteration of a FDLF to estimate the state of the system after a contingency outage. Eigenvalues from the first iteration of an iterative eigenvalue computation were used to approximate the system eigenvalues (and hence estimate the worst damped eigenvalues) during the disturbance. From the results presented, accurate ranking of the contingency list was achieved and the computation time was greatly reduced, since only those cases at the top of the ranked list required further dynamic stability eigenvalue analysis.

2.4.2 Artificial Intelligence Applied to ACS

Recent developments in automatic contingency selection and security analysis have encompassed the techniques of artificial intelligence. These are primarily rule-based or expert systems and neural network applications.

2.4.2.1 Expert Systems

Christie et al. [38] introduced the concept of expert systems (ES) to on-line security assessment. They discussed that contingency selection and the subsequent analysis of the results were essentially data-driven processes, so that expert systems were well suited to this type of approach provided that the performance is comparable to that of a human expert and off-line studies which generate greater detailed assessments of the system state.

Sobajic et al. [39] developed a knowledge-based system for screening power system contingencies. This rule-base was built up from system operator experience and simulation models and was entirely independent of system size and complexity. The ES was designed to fulfil two main objectives, that of detecting and removing harmless contingencies from further processing and recognising potentially hazardous disturbances, together with the corresponding endangered areas of the system. Both single and multiple line outages were filtered by this mechanism in order to carry out a full ac load flow on the selected cases.

In a follow-up to [10], Christie developed the idea that security analysis could not be simply defined by a single PI, but required information about a number of other quantities, namely quality of supply, the potential loss of supply, the likelihood of quality loss as well as some mechanism to help the operator formulate corrective or

preventative actions. An expert system was introduced that attempted to collate and mimic operator knowledge used in off-line studies. However, it was suggested that new methods for capturing and adapting this information would have to be developed to keep up with future needs of a security assessment algorithm. In a later publication [40], Christie resolved many of the problems that were mentioned above by generalising the program to deal with security assessment information from a number of power utilities which differed only in detail rather than in its basic content. Future developments were outlined to implement a cooperative structure between expert system and algorithmic approaches (i.e. a hybrid approach) and, hence, providing a facility for expressing corrective actions as well as security analysis.

Fouad et al. [73] described a method where a Transient Energy Function (TEF) approach (which will be explained in the next chapter) could be used in security assessment. A rule-based system was used to process the results of the TEF. For a given contingency, the TEF method provided a measure of the stability margin and system sensitivity to changes in operating parameters. A multi-level tree structure for the expert system was implemented to deal with the decision making concerning the power system's security (from the stability margin) and its vulnerability (from the sensitivity margin) to external influences.

A fuzzy set approach (described in Chapter 4) was implemented by Hsu et al. [41] to efficiently rank contingencies. Post-contingent quantities from a fast decoupled load flow were categorised using fuzzy set notation. System operator experience and heuristic rules were represented linguistically by a set of fuzzy reasoning rules. By using these to analyse the post-contingent quantities, a ranked list of contingencies was produced. Tuning could be performed on these fuzzy representations to mimic operator performance in conducting contingency analysis.

2.4.2.2 Artificial Neural Networks

When examining the contingency selection and ranking problem, many researchers have discussed that it is essentially a pattern recognition technique in which contingencies that give undesirable network conditions are sought. This type of approach would seem well suited for artificial neural networks (ANN).

The interest in ANN applications to power system security started in earnest in the late-1980's, with Sobajic et al. [74] using a neural network to calculate fault clearing times (CCT) for post-fault dynamic studies. Various power network topologies and system loading conditions were used to train the ANN, so that it could be more adaptable in the on-line stage. Results in the literature showed that the estimated CCTs were comparable to those from analytical techniques.

Fischl et al. [75] developed a method by which neural networks could be used to detect "limiting contingencies" where lack of reactive power presents a problem in that real power transfers across the system have to be restricted. As with all ANN applications, once the network has been exhaustively trained with off-line studies (the problem is compounded with an increase in system size), the execution on-line is very fast.

El-Sharkawi et al. [76] used a similar technique for on-line static security analysis of power systems and trained a neural network on busbar voltages and line loadings as well as real and reactive power profiles. At each operating point, a set of optimal load flow equations were solved and the system security was determined and added to the training set. When running in an on-line mode the ANN displayed a security margin graphically showing the current operating point and its proximity to the security boundary.

Continuing the work in [77], Sobajic introduced a combined use of unsupervised and supervised learning criteria for the neural network, since it could then handle large volumes of data. A new unsupervised learning algorithm was developed for grouping large bodies of data on the basis of previously discovered similarities. A supervised learning mechanism was then used to calculate accurately the CCT from these groups.

Fouad et al. [78] applied an ANN to the concept of power system vulnerability, using the results from a TEF as the inputs to the neural network, i.e. stability margin and system sensitivity. The ANN was trained to produce outputs of unity for a vulnerable system and zero otherwise.

2.4.2.3 Hybrid Approaches

Recent developments [42] have involved combining the relative powers of expert systems and neural networks to a complete security assessment algorithm. An ES was used to screen and select potentially severe contingencies, with the resultant list corresponding closely to that picked by a human expert. An ANN was applied to determine definitely stable and potentially unstable contingencies after fault clearing, showing a high level of accuracy and reliability. Also discussed in [42], artificial intelligence techniques can be useful for input data management and interpreting the security assessor results in a linguistic form for system operators.

2.5 Chapter Summary

The subject of power system security assessment has been described in this chapter with distinctions made concerning security and contingency analysis. The concept of automatic contingency selection has been introduced and its previous develop-

ments together with applications of artificial intelligence techniques in this area have also been discussed.

It is intended that an expert system based approach, namely a fuzzy set method, will be implemented, as part of this research, into a real-time power system simulator in order to carry out contingency analysis. This is together with power system stability analysis, which will now be the subject of the next chapter.

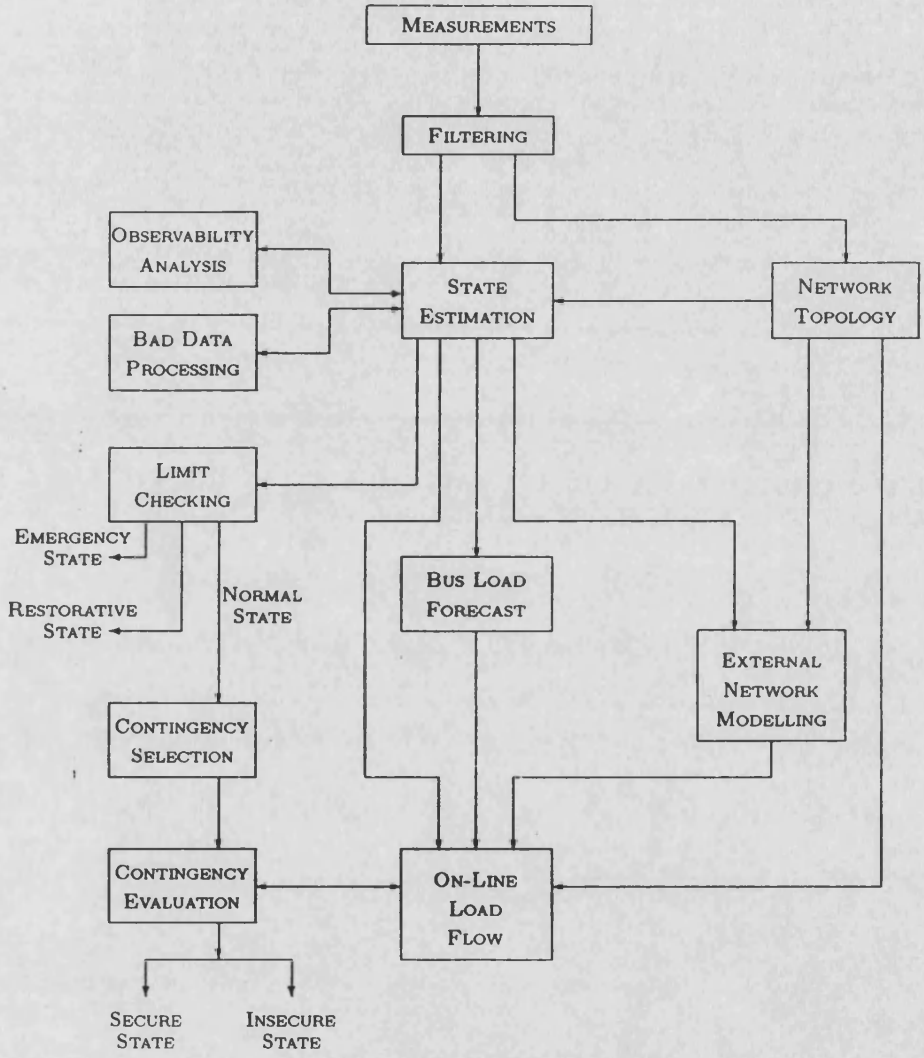


Figure 2.1: Main Components of an On-line Security Analysis Function

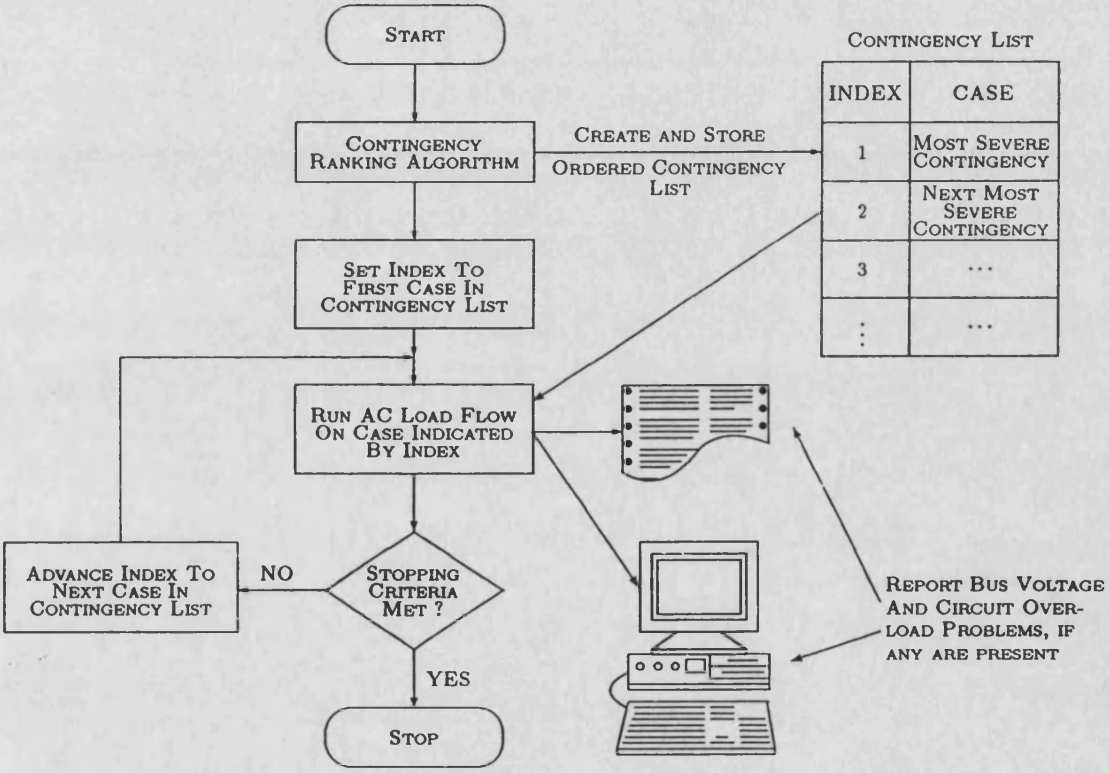


Figure 2.2: Typical Automatic Contingency Selection Algorithm

Chapter 3

System Stability and Violation Detection

3.1 Introduction

Power systems are examples of large non-linear systems with a wide range of stability problems where the areas of interest are, primarily, the behaviour of synchronous generators during a large system disturbance [2, 79–82]. In these stability studies, both the short-term dynamics of the initiating and subsequent (such as cascade tripping) events as well as the longer-term dynamics of the system should be simulated and analysed. Conventionally, *transient* stability programs are used to study the fast synchronising oscillations following a large disturbance, with a typical simulation duration of one to ten seconds. *Dynamic* stability algorithms ignore these fast machine oscillations and concentrate on the longer-term effects of slow power and voltage swings and frequency deviations, resulting from sustained energy imbalances, over a simulation time range of tens of minutes. The fundamental differences between each mode of oscillation will be explained in more detail in the next section, together with other modes of instability.

With any security analysis program and considering the size and complexity of a typical modern power system, an operator cannot expect to detect all abnormal conditions. An avalanche of warnings collected from around the system during and

after a disturbance will occur, such that the operator could not possibly process all the information. It is because of this very reason that alarm processors have been developed over the last decade to evaluate the importance of each message and hence focus the attention of the operator and help him to track the evolution of the state of the power system by providing a summary of the abnormal conditions. Various alarm handling approaches and their effectiveness to security assessment will be discussed in a further section.

3.2 Modes of Instability and Detection Mechanisms

The stability of a system of interconnected dynamic components is defined as its ability to return to normal or stable operation after some disturbance has been applied [2, 79].

There are principally two modes of instability in power systems: the loss of synchronism between synchronous machines and the stalling of asynchronous loads. Synchronous stability can itself be divided into further subgroups, *steady state* and *transient.*

Steady state, which is often referred to as dynamic stability, can be described as the capacity of the power system to retain synchronism, under a given load condition, when small disturbances, such as load or generation pattern changes and switching out of lines, are applied.

Transient stability, however, is concerned with sudden large changes to the network condition, which can be brought about by faults such as short-circuits. Generally, due to network topology changes, it can be assumed that the maximum power that

can be transmitted is less than that for the corresponding steady state condition.

The stability of an asynchronous load is controlled by the voltage across it and hence is referred to as *voltage stability.* An example is that if the voltage becomes lower than a critical value, induction motors may stall. In a power system, both synchronous and asynchronous instability may occur. Since the former is generally more probable, this will be described in greater detail than the latter.

3.2.1 Transient Stability

Present day trends in operating modern interconnected power systems have resulted in heavily loaded transmission networks and hence power transfers across critical boundaries, resulting in operation closer to steady state limits. Because of this, power networks can reach transient stability limits before steady state limits, meaning that operating limits can no longer be predicted in advance. This illustrates the need for more real-time analysis with fast transient methods, which not only rapidly advise the operator of a dangerous problem but provide him with some form of corrective action to restore the system back to a safer state. Researchers have investigated a number of possibilities over several years to achieve this which are primarily "direct methods" based on energy functions and, more recently, "pattern recognition techniques" and "expert systems". Time simulations give accurate results with better machine and network modelling but can prove too computationally demanding for real-time operation.

3.2.2 Direct Methods

These techniques can be split into four main areas : Transient Energy Function (TEF), Equal Area Criterion (EAC), Potential Energy Boundary Surface (PEBS)

method and Hybrid methods [83]. Each will now be discussed in more detail.

3.2.2.1 Transient Energy Function

Fouad et al [73, 84–87] used a function to describe the system *transient energy* which is calculated at the end of each disturbance period and compared with a *critical* or threshold value for transient stability. This difference is known as the *transient energy margin.* The transient energy is the energy which causes a generator to lose synchronism and separate from the rest of the system. It contains kinetic energy and potential energy components. The critical energy is the maximum value of potential energy at the predominant *unstable equilibrium point* (UEP) for a particular disturbance. If all the transient kinetic energy is converted into potential energy, the system is post-fault stable.

Hence the transient energy margin can be defined as

"the critical energy (or potential energy at the UEP) - the kinetic energy at the end of the disturbance".

If this value is greater than zero, the system is deemed to be stable but to be unstable if a negative solution is found. The benefits of this method are that a degree of stability can be given together with system vulnerability to a change in a system parameter. The main drawback is that, at present, it can only be used for first swing stability studies, but it can still provide useful information about the network condition after the transient.

3.2.2.2 Equal Area Criterion

Research has been carried out over a number of years into improving Liaponov functions and the well known EAC [88–90]. A new technique, the Extended EAC, which is a composite of these two methods has recently been developed [91–93]. The principle reduces the power network under study into an equivalent single machine and infinite busbar system and evaluates its robustness with respect to a given fault using the EAC.

Measures can be calculated from simple algebraic expressions to provide a stability margin for a particular fault clearance time and the critical clearance time for which this margin disappears, i.e. the stability-instability boundary is reached when the stability margin becomes zero.

This technique, therefore, is effective for sensitivity analysis and also provides a tool for corrective action formulation. From the results presented in [91], the reliability against time simulation is satisfactory but is limited by the use of simplified system modelling. Research, however, is continuing to include automatic voltage regulators (AVRs) and governors as part of the reduced system.

3.2.2.3 Potential Energy Boundary Surface Method

The concept of PEBS [94–96] is a theoretical boundary surface that can be defined as the potential energy of the system with respect to a *stable equilibrium point* (SEP). From each SEP, a "trajectory" is drawn in every direction in angular space, until the potential energy reaches a maximum. A number of these defines a PEBS.

During a fault, if a trajectory does not cross the PEBS, the fault clearance time

is assumed to be less than the critical clearance time and the system is stable. A method using an iterative solution of this technique has been developed [97] which narrows the time range from stable to unstable clearance times to yield an accurate measure of the critical clearance time for a given fault.

Although simplified models of generators and loads are used, this method provides consistent stability predictions. It should be noted that the role of fast methods should enhance, rather than replace time simulations, which have always been capable of handling detailed system models.

3.2.2.4 Hybrid Models

Techniques have been developed [98] which combine the direct method approach with time simulations. The advantages of this include more complex and detailed system models, calculation of critical clearing times and system sensitivities, and the ability to detect instability beyond the first swing. The underlying problem, however, is still that the time domain simulation occupies a substantial CPU usage. This, in part, can be resolved by parallel processing techniques [99–104] and by the use of faster processors which will be described in a later chapter.

3.2.2.5 Pattern Recognition and Expert Systems

Recent developments have been made in the application of expert system techniques to stability studies and rapid analysis of transients in power networks [18–20, 73]. Expert systems can be used to provide guidance in conducting stability studies and with the formulation of conclusions. The procedure includes a knowledge-base identifying key variables and characteristics in the form of logical rules ("If A Then B" format) which an inference engine processes. The rule-

base interfaces to the transient stability program and other application program outputs. The analysis of transient stability problems is indicative of an iterative solving process. Variations on this theme include decision trees and fuzzy sets. The latter will be described in the next chapter, since it is this type of approach that will be applied to this research.

Research into pattern recognition techniques or primarily Artificial Neural Networks has produced another alternative to solving this problem [78, 105–107]. Its main objective is to reduce computational requirements to a minimum, at the expense of elaborate off-line computations. A pattern vector containing all the significant system variables is defined and evaluated for a number of different operating conditions in order to generate a "training set". A process whereby the vector is dimensionally reduced to identify the most significant set of variables is often referred to as "feature extraction". The final mechanism is to determine a classifier function where any sample of system variables in the pattern vector can be classified very rapidly as stable or unstable.

3.2.3 Dynamic/Steady State Stability

Steady state or dynamic[1] stability violations has caused problems in power systems throughout the world. In several cases, the presence of long transmission lines connecting separate systems has been a predominant feature. When instability occurs, oscillations in the power transferred between regions start to increase which can either remain sustained or grow to dangerous levels, due to insufficient system damping, thereby causing generator plant and line tripping. This is referred to as *oscillatory* steady state instability. Another cause can be from inappropriate set-

[1]The definition of steady state or dynamic stability inherently depends on which literature is read. The latter is favoured by North American organisations, the former by European.

tings of generator controllers and, in particular, the gains of the AVRs. These can introduce negative damping into a system which would otherwise be stable. The condition where system variables are increasing or ramping against one another is called *aperiodic* steady state instability.

The study of steady state stability if often conducted by linear analysis where linearised models of the power network and synchronous machines with their associated controllers are used [108–113] to investigate the effects of small changes in, for example, system loading. State-space theory using eigenvalues and eigenvectors can provide good indications of instability but, because of the size and complexity of the systems to be analysed, the storage requirements for the state-space matrix become enormous and hence the task of finding the eigenvalues becomes tedious. Much of the research effort in the last two decades has concentrated on the development of more efficient eigenroutines [114–120] to calculate the most positive and hence unstable eigenvalues but, the problem still lies with the size of the multimachine power system and computation time.

Even though a linear approach is the most appropriate for analysing steady state instability, many power utilities still use conventional transient stability time domain programs to study this phenomenon. The complexity and size of a typical modern power system (and hence the accuracy of results which may be maintained) can be handled by time simulation approaches but the problems involved are inherently similar to those of transient stability techniques, i.e. CPU usage. With the ever increasing power of modern processors, however, real-time or faster than real-time operation can be achieved permitting several seconds or even minutes of simulation time to be run in only a few seconds of real-time.

An interesting new development is that of artificial intelligence applications. Neural

network [78] and expert systems [21] approaches have been applied to steady state stability analysis. The latter encompasses some of the reasoning behind fuzzy logic which will be discussed in the next chapter. Both methods attempt to model the human operator in terms of monitoring system loading and generation so that deductive reasoning can be performed to evaluate the degree of stability. Since results are comparable with those of the more conventional eigenvalue analysis but without the laborious computations, a development of this method will be used in this research.

3.2.4 Voltage Stability

Often associated with steady state stability, voltage stability is increasingly growing in importance as power systems are being operated closer to their stability limits. This is, in part, due to a growth in load without a corresponding increase in transmission capacity.

Black-outs caused by voltage instabilities can be influenced by a number of factors such as network disturbances consisting of transmission line, transformer or generator losses. The phenomenon of voltage collapse can similarly result from load tap-changers, current limiters of generators, load characteristics at low voltages and inadequate reactive power resources.

For voltage security analysis, load modelling is of paramount importance and the composite load model characteristics may for low voltages be different from those normally used for transient stability studies. For true voltage instability, at least part of the load must be of the constant MVA type (known as self-restoring). Loads that have a constituent part of static or voltage sensitive types contribute much less to instability problems.

Presently, load flow (static) and transient stability (time domain) programs are the most commonly used mechanisms in assessing voltage stability. These approaches can be classed as "point-wise", since they must be rerun for every operating condition and contingency [121–126]. Recently, "region-wise" methods have been developed which identify regions of voltage secure operating points [127–130]. This type of approach is more applicable for on-line voltage stability analysis.

As mentioned previously, time domain solutions are accurate in modelling events leading to voltage instability but are time consuming in terms of CPU usage and expert assistance is required to interpret results, since there is no measure of system sensitivity and stability. However, it is still the benchmark for other approaches and research is continuing to develop a hybrid method [131] which encompasses the speed and information output of the region-wise procedures with the accuracy of time-domain simulations.

3.2.5 Summary

This section has given an overview of power system stability, the terms used and the methods of analysing the different modes. It is proposed as part of a security assessment module that transient and steady state stability will be addressed by a hybrid combination of a time simulation and artificial intelligence. Voltage stability is a complex problem and, due to insufficient load characteristic representation, load tap changers and excitation limiters on generator models, it will not be implemented as part of this research.

3.3 Alarm Processing

Since the early-1980's, considerable interest has been shown in the area of alarm processing which is an inherent feature of an Energy Management System or EMS. A list of alarms presented to power system control engineers during a disturbance is usually difficult to interpret with in the order of hundreds to thousands of messages arriving in a short period of time. Engineers are not fully able to understand each piece of information as it is presented to them within the time constraints of real-time operation and, hence make a judgement as to the original cause of the problem. In this type of situation, an important alarm may be ignored, resulting in a difficulty in alleviating the fault and compensating other parts of the network.

With the emergence of expert system techniques, much research has been applied to this area and methods have been implemented which effectively model the behaviour of the human operator. By using existing alarm processing software and hardware, the information may be presented in the form of summarised messages which are in a more concise and comprehensible form.

3.3.1 Background

Before the onset of the computer based Supervisory Control and Data Acquisition (SCADA) systems in the 1960's, power dispatch centres were equiped with one-on-one data links which reported major alarms, such as circuit breaker status changes.

The following decade saw an increase in the number of status points which would be periodically scanned by the SCADA typically every two to ten seconds. In present day climates, control centres are typically monitoring of the order of tens

of thousands of sample points distributed around the power network. As a result of this explosion in data availability, new alarm handling functions were developed in order for the SCADA and EMS to keep pace with the ever expanding role of control centres.

Wollenberg was theoretically the first to conduct a study into alarm processing [22]. He outlined a number of areas in which the handling of warning messages coming from the EMS could be improved and presented an "intelligent alarm processor" or IAP which implemented these modifications. An early form of expert system was used with a rule-base containing rules of the form "*IF Alarm A AND Alarm B THEN issue Alarm C*". Test results were presented displaying a potential reduction in output alarms of 75 %. Work in this area substantially increased with improvements to the basic rule-base and the inference engine.

Amelink et al. [132] described three methods to alleviate excessive alarms during a system incident. The first was that of "Statically Adaptive Message Processing". This involved message routing (in which the system alarms are distributed across a network of operator terminals, hence sharing the load), alarm prioritization, acknowledging and segmenting (a process by which the alarms could be grouped in summaries). This would run continuously regardless of the state of the system. A second method, that of "Dynamically Adaptive Message Processing", ran to resolve the problem of the added message burdens during a system disturbance. The final concept was to utilise artificial intelligence techniques in order to improve the message presentation to the operator using summaries as mentioned above.

Tesch et al. [133] expanded on Wollenberg's original work by implementing their knowledge-based alarm processor as part of a real-time application to Wisconsin Electric's EMS. The concepts of forward and backward chaining rules (to form

hypotheses and to attempt to prove each hypothesis, respectively) were developed from Wollenberg's model to provide an efficient selection of rules during the inference process so that the SCADA alarms could be interpreted into concise linguistic messages.

Wollenberg et al. supplemented his earlier paper by developing the original IAP to an installation stage at Northern States Power Company [134]. Whilst in operation, a number of problems were highlighted by system operators concerning functionality, data-base requirements and communication with the existing EMS. The authors describe how these were resolved, together with further extensions to include advanced features such as a facility to check control actions before being executed by the operator, in order to prevent overloads, low voltages or ultimately customer load shedding.

During the last three years, additions to the basic model have been developed to deal with transmission and distribution systems (the latter with more protective devices) [26] and automatic fault analysis routines to provide the operator with either a precise location or the area in which the fault has occurred [27].

An object-orientated approach was applied by Dillon et al. [23] aiding the interface between the knowledge-base and the existing SCADA system. Dillon later extended this by implementing a neural network/expert system method [25] using decomposition into hierarchical and distributed heterogeneous objects in a parallel processing environment to more readily tackle the problems of system scalability and real-time response.

3.3.2 Alarm Processing Applied to Security Assessment

As yet, alarm handling techniques have not been applied to a security assessment module. However, their application to security assessment has two advantages, since not only will the operator receive a list of ranked contingencies but also their associated summarised alarms, illustrating areas where there are may be low voltage or line overload problems but, in addition, use of this technique would provide a facility from which a course of corrective or preventative actions to alleviate these problems could be formulated.

Hence, as recommended by Wollenberg [24], during a contingency application, there needs to be a mechanism which incorporates a number of important features. These can be summarised as : -

1. Alarm Screening - filtering out unimportant or routine alarms that would, otherwise, be a nuisance or distraction to the operator.

2. Alarm Combining - composing alarms in one of two forms :

   - Summary Message (giving the general area of the problem or possibly a trend).
   - Synthesis Message (explaining an existing problem or warning of a potentially dangerous situation).

3. Temporal Reasoning - a process by which alarms are monitored to ascertain whether they have been issued to the operator in the form of summary or synthesis messages or, in addition, if any expected alarms for a particular event have not appeared or have timed out (i.e. at the end of a contingency analysis cycle period).

4. Alarm Prioritization - ranking alarms according to their individual severity during either normal operation of the power system or contingency evaluation.

5. Corrective Actions - identifying problems and recommending ways to alleviate them in the form of simple linguistic instructions acceptable for operator interpretation.

6. Alarm Presentation - producing a user-friendly display.

Each of these functions should be performed during the evaluation time period allowed per contingency. Function 5 will not be addressed here, since work is currently being conducted in this area [135].

In order to carry out any alarm handling procedure, messages coming from the power system need to be categorised into groups of increasing severity. A formal classification of security levels used by many power utilities is shown in Figure 3.1 [136]. The removal of violations from Level 4, for example, requires the EMS to reschedule generation in order to bring the system back to Level 3. Further more, the EMS must perform additional rescheduling, which may incur loss of load, to return the system to Level 1 or 2. Levels 5 and 6 in this study will be combined to give a "composite" security level which will normally be initiated by a transient instability problem. These security levels represent normal power system operation, that is these are acceptable operational states and the choice of preferred level depends on the utility's overall economy vs. security policy[2] and its means for applying corrective real-time control.

[2]The overall aim of economy vs. security control is to operate the system at lowest cost, with the guaranteed avoidance or survival of emergency conditions. This, in essence, means operating the power system as close as possible to its security limits.

The alarm processing algorithm to be used is shown in Figure 3.2. This is a general model that has been developed over a number of years as described in Section 3.3.1. Its operation is as follows : -

1. From the *Input Phase*, the *Fuzzy Rule Database* is searched to find all the events in which, for example the opening of a circuit breaker might be expected to occur.

2. These rules then form the "skeleton" for the hypotheses which are created (this is known as the "inference engine") with their associated sets of expected alarms. Note that one rule may infer more than one hypothesis, hence promoting a form of competition.

3. The alarm processor enters the *Evaluator Phase*, where all of the current hypotheses are checked to see if any have reached a full score of expected alarm messages.

4. Each group of competing hypotheses is examined to ascertain whether it has "timed-out". Time-out periods for normal EMS functions are specified by the power utility and are generally of the order of minutes. In the case of a security assessor, this will be the duration of the contingency application. Therefore, if a group of competing hypotheses does not reach a full score, the whole competing group is removed and a message printed to the memory structure (associated with that contingency) showing the most likely hypothesis.

5. The alarm processor returns to its *Input Phase* to read the next message from the stream of alarms and classifies them in terms of security levels and area assignment.

6. The fuzzy rule database is again examined to see if any of the current alarm messages is expected for any of the existing hypotheses and a counter is incremented if this is true.

7. The process then reaches the evaluator and the whole procedure continues until a hypothesis has reached its full score of expected alarm messages. This hypothesis and all of its competing hypotheses are removed from the alarm list and stored in the memory structure for this contingency and the process returns to the input phase ready for the arrival of the next message.

3.3.3 Summary

This section has discussed an artificial intelligence approach to alarm processing in a power system EMS, highlighting the need for such a procedure and the research that has been conducted in this area.

An alarm processor would seem well suited to a complete security assessment module, since it can provide additional information to an operator as well as the ranked list of contingencies and, hence, help him to formulate corrective actions. Alarm security levels and a basic algorithm have been proposed, which have been implemented as part of this research

3.4 Chapter Summary

This chapter has addressed the two remaining areas of a security assessment algorithm. These are namely power system stability and its modes of operation and alarm processing.

A brief literature review of each of these areas has been given and it has been

proposed that artificial intelligence be used to implement the complete security assessor with a real-time power system simulator.

The next chapter will describe the type of artificial intelligence, or more specifically expert system to be used, with Chapter 5 describing the time-domain simulator upon which this will be based.

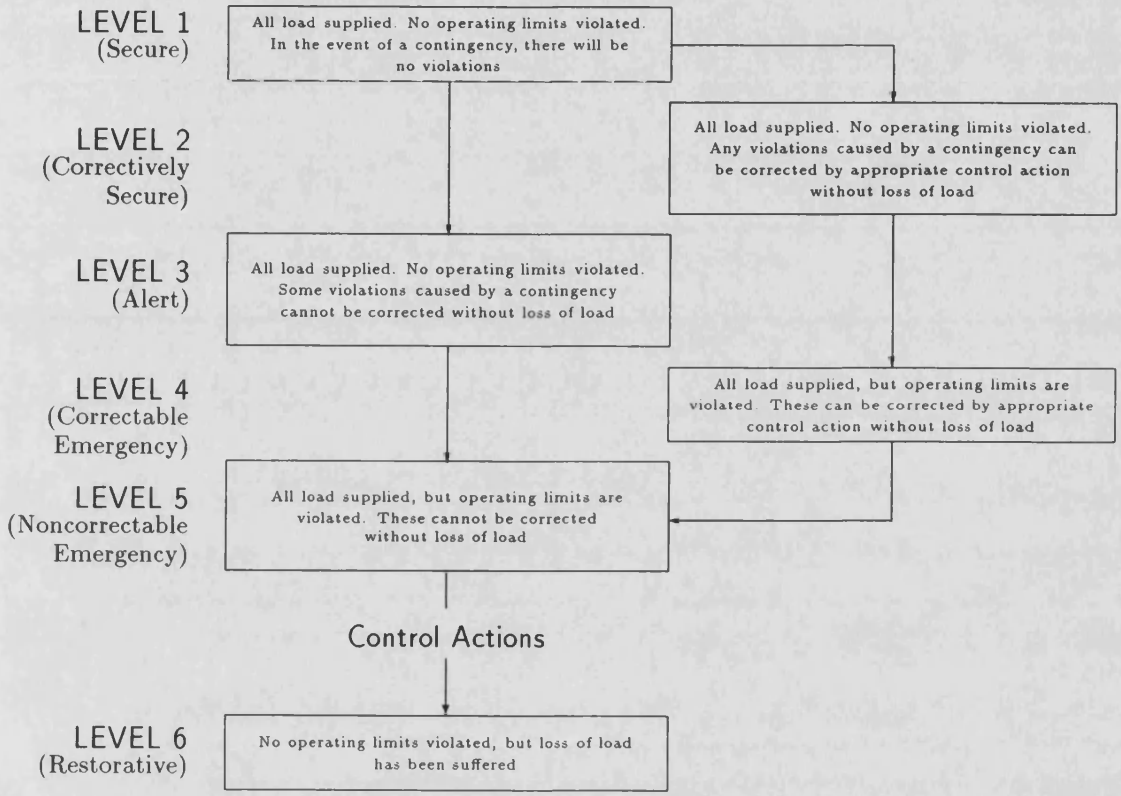


Figure 3.1: System Alarm Security Level Classification

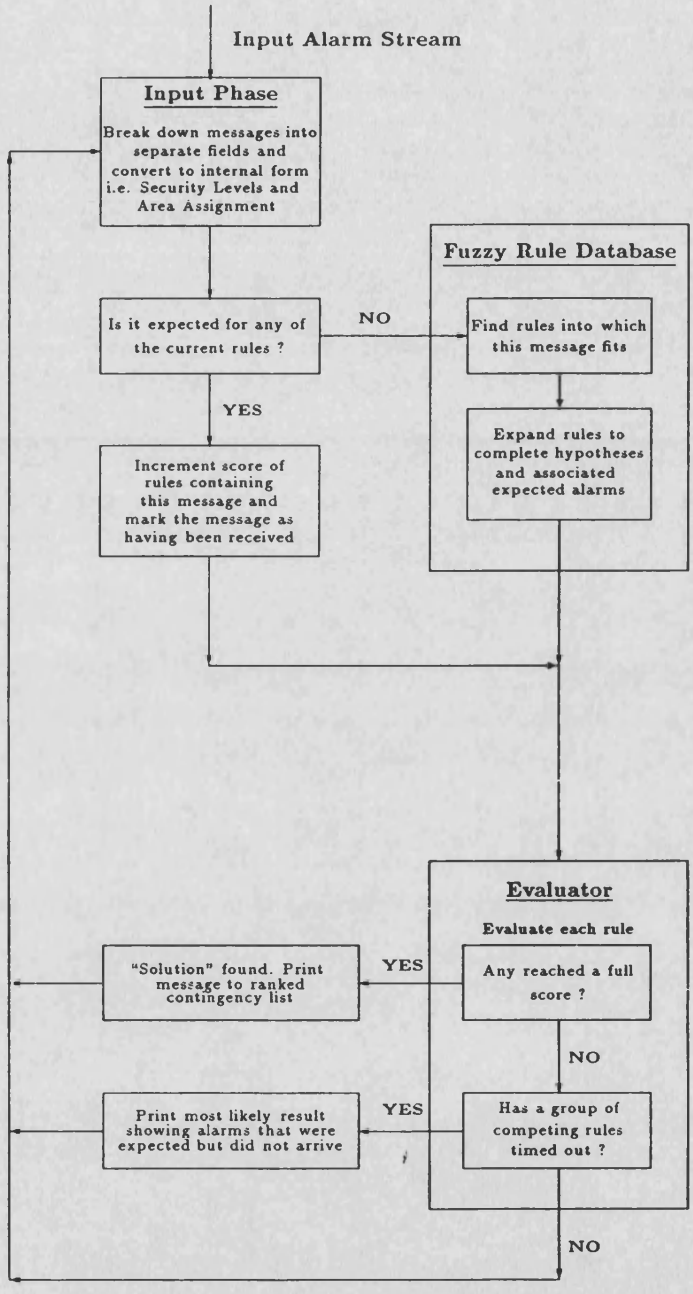


Figure 3.2: Alarm Processing Algorithm

Chapter 4

Fuzzy Logic

4.1 Introduction

Since the emergence of computing hardware and software in the late-1940's, traditional mathematical based methods applied to control theory have produced many quantitive tools and techniques. These have been derived from laws of mechanics, electromagnetism and thermodynamics and have been applied to controlling industrial processes which often rely heavily upon the existence of a mathematical model of how the process behaves. However, there are still some common processes which are not amenable to this type of treatment and to which mathematical theory cannot be successfully applied - in essence these are "humanistic systems". Within the literature, a number of authors have argued that rule-based systems for control differ fundamentally from the more traditional numerical techniques because they attempt to model the skills of the operator and not the process itself.

In this chapter, the problem of knowledge acquisition and how the role of fuzzy logic can be used to cope with an incomplete data-base will be discussed together with the application of fuzzy sets to deal with a non-linear system (an electrical power network) which moves gradually from one operating state to another rather than abruptly changing.

4.2 A History of Fuzzy Logic

L.A. Zadeh devised the initial premise of fuzzy set theory [49] in 1965. Since then, during nearly the past three decades, the fundamental notion of this field has been elaborated and has substantially matured. Most importantly, there has been considerable development of applications of fuzzy set theory to a wide range of problems.

4.2.1 Early Applications and Developments

The first article proposing the application of fuzzy set theory to control problems was that by Chang and Zadeh [137]. However it was the article by Zadeh [50] in 1973 on a "new approach to the analysis of complex systems and decision processes" describing the mechanism by which this type of approach could be used in a control environment that really formulated the theory upon which fuzzy controllers would be built.

During the mid-1970's, there was a significant increase in interest in the area of fuzzy controllers. The work of this initial period primarily focussed on the control of systems that were too difficult to model by more traditional methods. Mamdani and Assilian [138] published the first work in applying fuzzy set theory to the control of a small laboratory steam engine. Control was achieved with the use of linguistic rules to regulate heat and throttle settings in order to adjust engine speed and boiler steam setting. King and Mamdani [139], Larsen [140] and Tong [141] were among many who applied this early research to more complex industrial processes, see [142] for a complete bibliography.

In a non-industrial application of the fuzzy control model, Pappis and Mamdani

[143] described a fuzzy logic traffic controller for a single junction which, from the simulation results, proved more effective than other controller approaches.

4.2.2 Extensions to Fuzzy Control Theory

Using the same engine model [138], Mamdani developed a self-organising controller which permitted the learning of fuzzy rules of a process in a operating mode [144]. This demonstrated the strength of the self-organising approach even though a crude model was used. Procyk and Mamdani [145] later expanded on this same system.

Tong also applied fuzzy set theory to a fuzzy feedback system [146] in which he closed the loop around a controller to improve the stability of his fuzzy system, Cumani [147] further extended this approach.

The major new development in fuzzy set theory is in the move towards expert systems [148–153]. In the past, researchers have used the broader artificial intelligence approach of rule-based models rather than the fuzzy logic model. However, fuzzy control inference rules are quite similar to the inference rules used by an expert system and hence work in combining the two approaches is continuing.

Following on from Zadeh's initial work, there has been increased activity in the application of fuzzy programming techniques to control systems in robots. The Japanese/Americans seem to have excelled in this area, even extending this to fuzzy semi-conductor devices [154–156] in which the MC143150 Fuzzy Logic and Neuron chip has been used to control the flow rate and temperature of a fluid from one storage tank to another. Again, although this is a relatively small control system, application of a complete fuzzy tool has proved to be more efficient than

a more traditional controller of this type.

4.2.3 Summary

In a Siemens review paper [157], Reinfrank explained the current trend in research and development throughout the world into fuzzy set theory. Since the conception of this technique in the mid-1960's, work progressed in the US for the next decade. The Japanese showed no interest in the subject until the mid-1980's. Since then the explosion of fuzzy products developed in the Far East has been enormous, so much so that Reinfrank expressed concern as to whether Europe and the US could make up the divide that the Japanese have in both techniques, experience and market share.

4.3 Methodology

The principle behind fuzzy logic is to represent humanistic knowledge in a form recognisable to both man and machine. An operator may have a theory about what is the best thing to do whilst controlling a process and may express it using a rule of the type

"If x is small and x increases slightly Then y will increase slightly"

This contains several vague terms but it can be represented using fuzzy logic. This section will give a brief introduction to some of the terms used and will also describe the mathematical theory devised by Zadeh [50].

4.3.1 Overview

The method of describing a rule such as that above can be split into three distinct subgroups, as mentioned by Zadeh. These are principally

- *Linguistic Variables* which are used in place of numerical variables and are statements which have values described in some natural language, e.g. *size* can be classed as a linguistic variable which has values *very large*, *large*, *not large*, etc ...
- *Fuzzy Conditional Statements* which equate simple relations between variables. These are expressions of the form "**If** A **Then** B", where A and B have fuzzy meaning or alternatively are labels of fuzzy sets of the type

  If x is *small* **Then** y is *large*

- *Fuzzy Algorithms* can be used to equate more complex relations. These are a sequence of instructions which may contain fuzzy assignment and conditional statements. Figure 4.1 shows a typical fuzzy algorithm.

Efstathiou in her review paper [158] describes neatly how fuzzy set theory can be explained in "lay-man" terms. If the example of the linguistic variable *size* is used here, terms such as *small*, *medium* and *large* can be employed to describe the variable *size* on a linear scale, as in Figure 4.2.

For each term there will be a range of sizes which will definitely apply - this is known as its grade of membership (μ) and will appear in the set of 1. For the range over which the term does not apply, its grade of membership is in the set of 0. So far this has just mimicked traditional set theory which, in essence,

abruptly divides the grades of membership, i.e. either 1 or 0, True or False as in Figure 4.3. However, fuzzy set theory dictates that there is a region where the *size* variable does not cover the full scale and this will have a grade of membership somewhere between 0 and 1. Researchers, as in Figure 4.2, have terms describing their linguistic variables overlapping, so that there will be some cases where there will be more than one term at any time that will have a non-zero membership function.

Rules, such as that used at the start of this section, contain both a proportional (P) and a derivative (D) term, upon which most fuzzy logic controllers are based. To ease computation, the scales are often quantised and the resultant PD plane is made up of a finite number of grid squares, as in Figure 4.4.

Efstathiou remarks that to cover each square with a rule may be impossible for the operator and, for more complex systems, a very large number of rules would be required. It is also pointed out that fuzzy logic helps in the area of filling the knowledge base and dealing with the imprecision of the operator, so that "*the fuzziness in the definitions means that any fuzzy rule will have a region of influence*". In other words, due to the overlap between linguistic variable terms, there will be squares where more than one rule applies. A combination of these will fill in the blanks and when modified by the "degree of fulfillment" of each rule, the controller action should vary smoothly across the PD plane.

4.3.2 Mathematical Theory

As mentioned in Section 4.3.1, Zadeh defined three main subgroups. The methodology is based, in essence, around set theory and a brief explanation of the notation, operations and how linguistic variables, fuzzy conditional statements

and fuzzy algorithms are manipulated will be given.

4.3.2.1 Notation

A fuzzy subset **A** of a universal discourse **U** is characterised by a membership function

$$\mu_{\mathbf{A}} : \mathbf{U} \rightarrow [0,1] \tag{4.1}$$

This relates each member x in **U** to a number $\mu_{\mathbf{A}}$ in the interval 0 to 1 (denoted [0,1]), i.e. $0 \leq \mu_{\mathbf{A}} \leq 1$. This, therefore, represents the grade of membership of x in the subset **A**. It should be noted that the term fuzzy subset is used, **A** is a subset of **B**, when $\mu_{\mathbf{A}}(x) \leq \mu_{\mathbf{B}}(x)$ for all elements of x in the universe **U**.

Zadeh defines the *support* of **A** as a set of points in **U** where $\mu_{\mathbf{A}}(x)$ is positive and it follows that the *crossover point* in **A** is where $\mu_{\mathbf{A}}(x)$ is 0.5. A *fuzzy singleton* can be defined as a fuzzy set whose support is a single point in **U**. Thus if **A** is a fuzzy singleton whose support is a point x

$$\mathbf{A} \equiv \mu/x \tag{4.2}$$

where μ is the grade of membership of x in **A**. A fuzzy set is, therefore, the "union" of its fuzzy singletons

$$\mathbf{A} \equiv \int_{\mathbf{U}} \mu_{\mathbf{A}}(x)/x \tag{4.3}$$

so that for a finite number of singletons

$$\mathbf{A} \equiv \sum_{i=1}^{n} \mu_i/x_i \tag{4.4}$$

Note an arbitrary fuzzy subset of the universe **U** over the *continuum* is written in the form of an integral in Equation 4.3, where the term continuum refers to a set of real numbers. As an example, from Zadeh's paper [50], if the fuzzy set **A** is

labelled *Large*

$$\begin{aligned} Large &\equiv \int_7^{10} \mu_{Large}(x)/x \\ &\equiv \int_7^8 [\frac{(x-7)^2}{2}]/2 + \int_8^9 [1 - \frac{(x-9)^2}{2}]/2 + \int_9^{10} 1/x \end{aligned}$$

For example, if **A** is the fuzzy set *Viscosity* in the universal discourse **U**, such that **U** = *Water + Oil + Ink + Tar*,

$$Viscosity \equiv \frac{low}{Water} + \frac{medium}{Oil} + \frac{low}{Ink} + \frac{high}{Tar}$$

where *low*, *medium* and *high* are grades of membership acting as fuzzy sets in the universe **U**.

4.3.2.2 Fuzzy Relations

A fuzzy *relation* **R** from a set **X** to a set **Y** is a fuzzy subset of the Cartesian product $\mathbf{X} \times \mathbf{Y}$, where $\mathbf{X} \times \mathbf{Y}$ is a collection of ordered pairs or binary variables (x, y), $x \in \mathbf{X}$, $y \in \mathbf{Y}$. Hence, **R** is described by a "double" membership function $\mu_{\mathbf{R}}(x, y)$ and can be expressed in a similar way to Equation 4.3, i.e.

$$\mathbf{R} \equiv \int_{\mathbf{X} \times \mathbf{Y}} \mu_{\mathbf{R}}(x, y)/(x, y) \tag{4.5}$$

As an example, if $\mathbf{X} = \{Black,\ Golden\}$ and $\mathbf{Y} = \{Dog,\ Fish,\ Bird\}$, the Cartesian product of $\mathbf{X} \times \mathbf{Y}$ is given by

$$\begin{aligned} \mathbf{X} \times \mathbf{Y} \equiv\ & \{(Black,Dog),\ (Black,Fish),\ (Black,Bird), \\ & (Golden,Dog),\ (Golden,Fish),\ (Golden,Bird)\} \end{aligned}$$

If the fuzzy relation **R** is defined as **R** = *Likes Four-Legged Animals*

$$\mathbf{R} \equiv \{0.8/(Black,Dog),\ 0.3/(Golden,Dog)\}$$

where 0.8 and 0.3 are some arbitrarily chosen grades of membership of the set *Likes Four-Legged Animals*, indicating that the person prefers black dogs to golden dogs.

Similarly for $\mathbf{R}$ = *Likes Legged Animals*

$$\begin{aligned}\mathbf{R} \equiv\ & \{0.8/(Black,Dog),\ 0.3/(Golden,Dog),\\ & 0.2/(Black,Bird),\ 0.7/(Golden,Bird)\}\end{aligned}$$

This relationship is usually expressed as a *relation matrix* in which the $(i,j)^{th}$ element is the value of $\mu_{\mathbf{R}}(x,y)$ for the i^{th} value of x and the j^{th} value of y respectively, so that

$$\begin{array}{c} \\ Black \\ Golden \end{array} \begin{array}{c} \begin{array}{cc} Dog & Bird \end{array} \\ \begin{bmatrix} 0.8 & 0.2 \\ 0.3 & 0.7 \end{bmatrix} \end{array}$$

The *composition* of two fuzzy relations $\mathbf{R}$ ($\mathbf{X}$ to $\mathbf{Y}$) and $\mathbf{S}$ ($\mathbf{Y}$ to $\mathbf{Z}$) can be defined as

$$\mathbf{R} \circ \mathbf{S} \equiv \int_{\mathbf{X}\times\mathbf{Z}} \vee(\mu_{\mathbf{R}}(x,y) \wedge \mu_{\mathbf{S}}(y,z))/(x,z) \tag{4.6}$$

from which the max ($\vee$) - min ($\wedge$) rules are derived, thus : -

$$a \vee b = max(a,b) \equiv \begin{cases} a, & \text{if a} \geq \text{b} \\ b, & \text{if a} < \text{b} \end{cases} \tag{4.7}$$

$$a \wedge b = min(a,b) \equiv \begin{cases} a, & \text{if a} \leq \text{b} \\ b, & \text{if a} > \text{b} \end{cases} \tag{4.8}$$

4.3.2.3 Fuzzy Set Operations

As with any set theory, there are a number of operations that can be carried out. The negation *not*, connectives *and* and *or* and other terms such as the linguistic

hedges *very*, *more or less*, etc ... can be described by these operations in fuzzy set notation.

- *Complement* of **A** is indicated as $\neg$ **A** where

$$\neg \mathbf{A} \equiv \int_{\mathbf{U}} (1 - \mu_{\mathbf{A}}(y)) \; / \; y$$

- *Union* of **A** and **B** is indicated as **A** + **B** where

$$\mathbf{A} + \mathbf{B} \equiv \int_{\mathbf{U}} (\mu_{\mathbf{A}}(y) \vee \mu_{\mathbf{B}}(y)) \; / \; y$$

  This is equivalent to the use of the connective *or* such that

$$\mathbf{A} + \mathbf{B} \equiv \mathbf{A} \text{ or } \mathbf{B}$$

- *Intersection* of **A** and **B** is indicated as **A** $\cap$ **B** where

$$\mathbf{A} \cap \mathbf{B} \equiv \int_{\mathbf{U}} (\mu_{\mathbf{A}}(y) \wedge \mu_{\mathbf{B}}(y)) \; / \; y$$

  This is equivalent to the use of the connective *and* such that

$$\mathbf{A} \cap \mathbf{B} \equiv \mathbf{A} \text{ and } \mathbf{B}$$

- *Product* of **A** and **B** is indicated as **AB** where

$$\mathbf{AB} \equiv \int_{\mathbf{U}} (\mu_{\mathbf{A}}(y) \; \mu_{\mathbf{B}}(y)) \; / \; y$$

  from which the relations can be calculated

$$\mathbf{A}^{\alpha} \equiv \int_{\mathbf{U}} (\mu_{\mathbf{A}}(y))^{\alpha} \; / \; y$$

$$\alpha\mathbf{A} \equiv \int_{\mathbf{U}} \alpha \; (\mu_{\mathbf{A}}(\mathrm{y})) \; / \; y$$

- *Concentration* of **A** is indicated by *CON* (**A**) where

$$CON\,(\mathbf{A}) \equiv \mathbf{A}^2$$

  This has the effect of reducing the magnitude of the grades of membership of x in **A**, slightly for high μ's and greatly for low μ's.

- *Dilation* of A is indicated by $DIL\ (\mathbf{A})$ where

$$DIL\ (\mathbf{A}) \equiv \mathbf{A}^{1/2}$$

This has the opposite effect to the *Concentration* operation above

- *Contrast Intensification* is indicated by $INT\ (\mathbf{A})$ where

$$INT\ (\mathbf{A}) \equiv \begin{cases} 2\mathbf{A}^2, & \text{if } 0 \leq \mu_{\mathbf{A}}(x) \leq 0.5 \\ \neg 2(\neg \mathbf{A})^2, & \text{if } 0.5 \leq \mu_{\mathbf{A}}(x) \leq 1.0 \end{cases}$$

Again, this is similar to the operation of *Concentration* in that it increases the values of $\mu_{\mathbf{A}}(x)$ which are above 0.5 and reduces those below this point. This has the effect of reducing the *fuzziness* of **A**.

Other operations are described in more detail in [50, 51, 159–161].

4.3.2.4 Hedges and Linguistic Variable Interpretations

An important application of fuzzy sets is in "computational linguistics" whose aim is to calculate with natural language statements in a similar way as logic calculates with logical statements. Fuzzy sets and *Linguistic Variables* can be used to determine the meaning of this natural language, which can then be manipulated. A linguistic variable is assigned values which are expressions such as words, phrases or sentences. For example, from Section 4.3.1, the linguistic variable *size* has values *small*, *medium* and *large*. Although it is possible to define values for the size *small*, these will be very subjective in nature.

Zadeh suggests that a value of a linguistic variable is a composite term which can be divided into four groups : -

1. Primary terms, i.e. labels of fuzzy subsets of the universal discourse.

2. The negation *not* and the connectives *and* and *or.*

3. Hedges, such as *very, more or less*, etc ...

4. Markers, such as parentheses.

Hedges are another definition of a fuzzy set and serve to modify the meaning of this set. Thus, a larger set of values will be generated for any particular linguistic variable. For example, the *size* fuzzy set could be defined as : -

$$\begin{aligned} size \;=\; & very\ small + very\ very\ small + more\ or\ less\ small + \\ & not\ very\ small + ... \end{aligned}$$

The hedges mentioned above, i.e. *very, more or less*, etc ..., are usually defined in terms of fuzzy set operations, so that

$$\begin{array}{lcl} very\ small & \equiv & CON\,(small) = small^2 \\ very\ very\ small & \equiv & CON[CON(small)] = small^4 \\ more\ or\ less\ small & \equiv & DIL\,(small) = small^{1/2} \\ not\ small & \equiv & 1 - small \\ not\ very\ small & \equiv & 1 - CON(small) \end{array}$$

4.3.2.5 Fuzzy Conditional Statements

Using the expression "*If x is small Then y is large*" as an example of a *Fuzzy Conditional Statement*, the term "*x is small*" is the antecedent and "*y is large*" is the consequent. Zadeh suggests that a statement of this kind describes a relation between two fuzzy variables and that a fuzzy conditional statement can be defined as a fuzzy relation as in Equation 4.5. Hence the Cartesian product of two fuzzy subsets **A** and **B** in the universes of **U** and **V** respectively is : -

$$\mathbf{A} \times \mathbf{B} \equiv \int_{\mathbf{U} \times \mathbf{V}} (\mu_{\mathbf{A}}(u) \wedge \mu_{\mathbf{B}}(v))/(u, v) \qquad (4.9)$$

where $\mathbf{U} \times \mathbf{V}$ is the Cartesian product of the non fuzzy sets **U** and **V**. Therefore, $\mathbf{A} \times \mathbf{B}$ is a fuzzy relation from **U** to **V**, so that, in general form : -

$$\textit{If } \mathbf{A} \textit{ Then } \mathbf{B} \equiv (\mathbf{A} \times \mathbf{B})$$

In cases where the operand "*Else*" and a third fuzzy subset **C** are introduced, the Cartesian product is : -

$$\textit{If } \mathbf{A} \textit{ Then } \mathbf{B} \textit{ Else } \mathbf{C} \equiv (\mathbf{A} \times \mathbf{B}) + (\neg\mathbf{A} \times \mathbf{C})$$

where "+" is the union of the fuzzy relations $(\mathbf{A} \times \mathbf{B})$ and $(\neg\mathbf{A} \times \mathbf{C})$.

The *Compositional Rule of Inference* is based on the composite rule, as in Equation 4.6, so that if **R** is a fuzzy relation from **A** to **B** and x is a fuzzy subset of **A**, the fuzzy subset of y of **B** which is "induced" by x is given by the composition of **R** and x, i.e.

$$y \equiv x \circ \mathbf{R} \tag{4.10}$$

so that y is given by the max-min product of x and **R**. In the example used by Zadeh

a) *x is very small*
b) *If x is small Then y is large Else y is not very large*

a question arose as what would the value of y be when x is *very small.* Substituting the values of *small* for **A**, *large* for **B** and *not very large* for **C** in the conditional statement $(\mathbf{A} \times \mathbf{B}) + (\neg\mathbf{A} \times \mathbf{C})$, the relation matrix **R** describing this fuzzy conditional statement could be built up. The result of the composition of **R** and substituting the value of $x =$ *very small* yielded the value of y for this condition.

4.3.2.6 Fuzzy Algorithms

As mentioned previously, a *Fuzzy Algorithm* is a sequence of ordered instructions which a controller may use to operate a process. It is, in essence, an example of how humans behave either consciously or subconsciously in every day life. Combining the concepts of linguistic variables and fuzzy set operations to yield fuzzy conditional statements, fuzzy algorithms can be seen to approximate analysis systems or decision processes much as a human would but, at a level too complex for a purely mathematical technique to cope with.

Zadeh suggested that these ordered instructions (fuzzy or not) would fall into one of three categories : -

1. Assignment statements, such as *x is small*, *x is not large and not very small*, etc ...
2. Fuzzy conditional statements, such as *If x is small Then y is large Else y is not large*, *If x is small Then go to 7*, etc ...
3. Unconditional action statements, such as *decrease x slightly*, *print x*, etc ...

where a combination of each of these is executed by the compositional rule in Equation 4.9. Cases where two conflicting alternatives arise from the execution of the algorithm, a *Rule of Preponderant Alternative* is used to decide which of the courses of action should be taken based on which is more true than the other. If both alternatives have more or less equal truth values, the choice can be made arbitrarily.

A number of algorithm classifications are described in [50, 51], each corresponding

to a particular type of application and briefly include : -

- *Definitional and Identificational Algorithms.* The former is a finite set of fuzzy instructions which define a fuzzy set in terms of other fuzzy sets. The latter calculates the grade of membership of any element of the universal discourse in the set under definition, i.e. decides whether an element belongs to a particular set or not.
- *Generational Algorithms.* These serve to generate rather than define fuzzy sets.
- *Relational and Behavioural Algorithms.* The former describes relations between fuzzy variables, whereas the latter describes the approximate behaviour of a process or system.
- *Decisional Algorithms.* These provide an approximate description of a decision rule.

It should also be noted that algorithms, of the form mentioned above, may contain a number of other types of algorithm which are often referred to as sub-algorithms.

4.3.3 Summary

This section has shown that by using Zadeh's linguistic variable and fuzzy algorithm definitions, a method can be developed for describing a system that is either too complex or too ill-defined, as expected from a humanistic function (which is not governed by crisp boundaries), to be controlled by a mathematical algorithm. The approach may only be approximate but it has proved its efficiency in dealing with animate rather than inanimate behaviour.

4.4 Applications to Power Systems

A power system consisting of a number of generating plants, busbars and transmission lines exhibits a high order of non-linearity. Because of its very nature, fuzzy set theory would seem to be directly applicable to the analysis and control of power systems.

Until recently, however, work in this area has been rather limited but, because of the constraints now imposed upon most power utilities throughout the world due to economic and environmental reasons, there is increased interest in the subject of expert systems (and also fuzzy logic) in running power networks more efficiently, even though this may entail on-line operation near to stability limits.

The fuzzy set theory approach has been applied in one form or another to a range of power system problems which control staff deal with on a day to day basis. This is in part due to the lack of any procedure in human decision making such that a mathematical mechanism could simply not cope.

4.4.1 Previous Applications of Fuzzy Set Theory

4.4.1.1 Demand and Generation Control

The first real work conducted into solving power system problems was in the late-1970's, in which Dhar [162] applied fuzzy concepts to the decision making process in planning a long-term generation and transmission schedule. The fuzzy environment was created from the unknown or imprecise system states such as demand patterns and generation and fuel resources. It was argued that this was a valid approach, since traditional statistical methods would inheritantly lead to

inaccurate results due to the unpredictable objectives and constraints used in this time frame. Fuzzy sets together with linguistic variables were employed to represent different criteria of merits (for example capital expenditure), resulting in optimal alternatives for these different criteria which were effectively ranked against one another.

Economakos limited his research to power demand forecasting and loading of a power system [163]. He used fuzzy techniques to study situations where, although statistical data was available, there were certain load patterns which were not precisely defined or rather vague and were based purely on either operator experience or common sense. Three load components or fuzzy sets were used, principally domestic, industrial and street lighting demand, which were divided into ten linguistic variables over a twenty four hour period. These yielded membership functions for each load component per hour time span. Given the maximum forecasted demands in MW and MVAr from historical data, all possible loading conditions for each component and hence the total system load could be predicted in the same way as an experienced operator. The advantage that this technique has over a human expert is that the composition of each load component allows for the judgement of how likely the scenario is to occur. Hsu later expanded on this idea, extending it to provide a guide for service restoration in the case of load shedding [164].

4.4.1.2 Stability Analysis

A number of researchers have applied fuzzy techniques to predicting power system instability. The concepts of stability have already been described in Chapter 3, so only the application will be discussed.

Souflis et al. [165] produced a transient stability index that provided an evaluation of the system security level by taking into account generator acceleration and kinetic energy during a large disturbance. Six fuzzy sets were used with five linguistic variable terms describing these quantities. Relation matrix manipulations were carried out to yield a stability decision which is presented to an operator in a linguistic manner. A conclusion was drawn stating that this fuzzy approach could be made in a fast manner and by merely adjusting the "weights" of the linguistic variables, the derivation of the stability index was sufficiently flexible and adaptable to analyse any system.

A fuzzy set approach was applied by Hsu et al. [21] to provide an operational aid to steady state stability. Five fuzzy sets were used to describe inter-area line flow and generator output upon which a set of fuzzy-expert rules were applied. Membership functions were calculated from these to give a measure of the system stability and categorised in one of four regions. Hence the pseudo fuzzy-expert system would perform deductive reasoning on the degree of steady-state stability. The authors concluded that this was indeed much faster than a conventional method which would otherwise require complex eigenvalue computations.

4.4.1.3 Contingency Ranking

Hsu went on to apply fuzzy set theory to contingency ranking [41]. Here operator experience and "heuristic" knowledge were used to represent post-fault line flows and busbar voltage magnitudes with the aid of fuzzy sets. A loadflow was used to calculate the post-contingent quantities which were classified in one of the fuzzy sets. Again manipulating relation matrices yielded an overall system severity index per contingency which could then be ranked. Hsu concluded that by conducting fuzzy reasoning on these sets and with input from the expert to tune the fuzzy

parameters, the approach could mimic an experienced operator in conducting contingency ranking.

4.4.2 Proposal for the use of Fuzzy Sets in Dynamic Security Assessment of the British National Grid

The National Grid Company plc operates a large integrated transmission system, covering England and Wales. This comprises of at least 500 circuits of overhead lines and cables at 400 and 275 kV, connecting 250 generators to 170 supergrid supply points.

The system is planned to be operated economically and securely at all times. Economy in this case means running the cheapest generators first according to a merit order table. However, security will over-rule this and is interpreted to mean that no circuit flow may exceed its thermal rating following any credible fault.

Therefore, it is proposed that fuzzy set theory will be applied to a real-time simulation of the National Grid system to provide on-line advice to an operator in areas of contingency ranking and analysis, alarm processing and system stability assessment. The effect of economy will effectively be ignored in this thesis as all generators will be assumed to be "in-merit".

4.5 Chapter Summary

This chapter has addressed three main areas - a brief review of the work that has been conducted and the developments made to the basic fuzzy set theory, an introduction to the methodology in verbal and mathematical nomenclature and an insight into the way in which researchers have tackled power system based

problems. A proposal has also been made to apply these techniques to give security assessment advice on a real-time simulation of the National Grid system.

The next chapters will describe the need for simulation in the study of these proposals and how the simulator has been developed for this work.

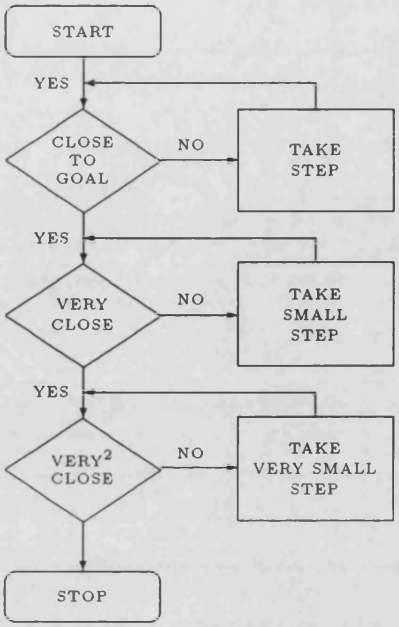


Figure 4.1: An Example of a Fuzzy Algorithm

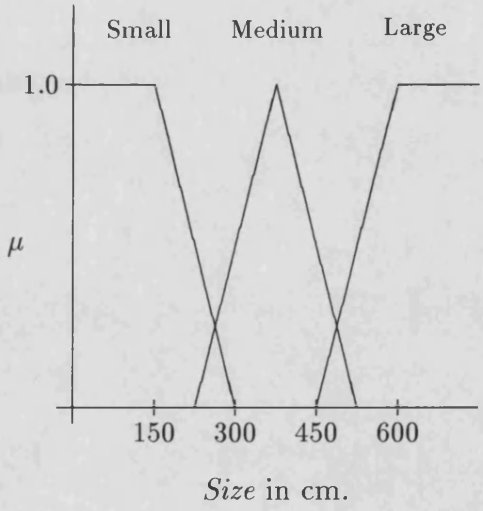


Figure 4.2: Plot of Fuzzy Membership Function μ against Linguistic Variable *Size*

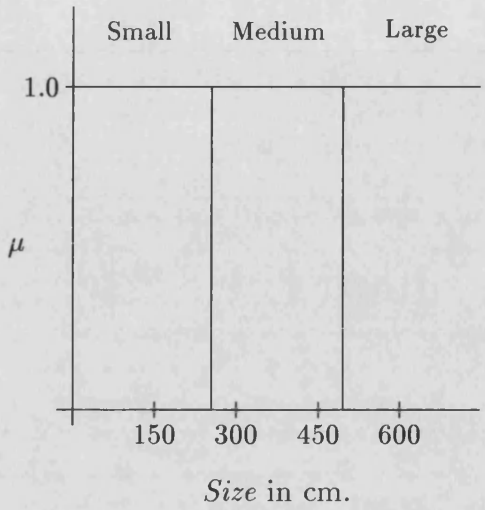


Figure 4.3: Plot of Normalised Membership Function μ against Linguistic Variable *Size*

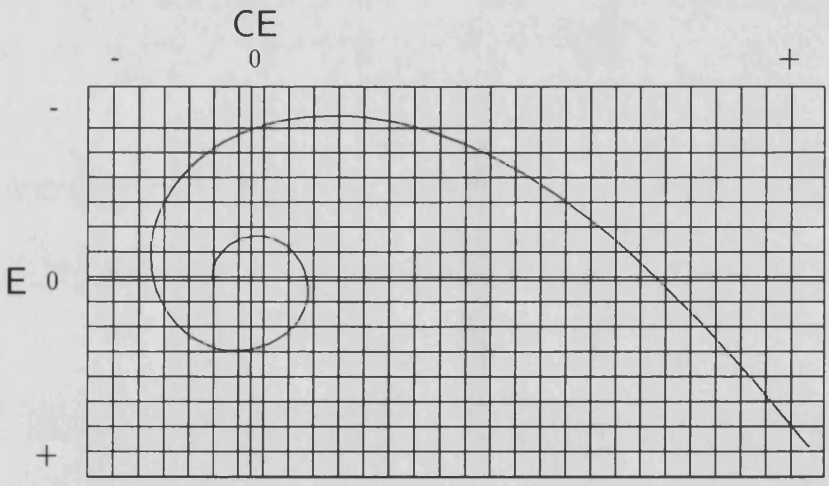


Figure 4.4: PD Control Plane for a Simple Fuzzy Rule-Based Controller

Chapter 5

Power System Simulation

5.1 Introduction

Simulators designed to evaluate the performance of power systems have been available for many years. They first existed in the form of analogue computers and, more recently, simulations have been run on digital computers in both the *batch* and *interactive* modes.

The modern power system planning engineer finds the design task is simplified by the presence of an appropriate simulation of the existing and proposed system being modelled, which runs accurately on a workstation available in the office. However, the availability of good interaction does not require that the simulation runs in real-time nor that the workstation provides advanced animated graphics.

In the case of the power system operator, the requirements will be somewhat different. A simplified network model can be used in many cases but animated graphics displaying both the steady-state and the transient behaviour of the system in real-time has rapidly become a preferred analytical tool. An important aspect of the use of this form of simulator is as a training tool where the trainee operator can subject the model power system to a range of disturbances and potential remedies in a manner which would be totally unacceptable on the real

system due to constraints such as time, cost and safety.

This leads to two concepts : *hard real-time*, where the solution time will be equal to the model time step under all conditions without losing synchronism with the real (clock) time and, *soft real-time*, where the solution time will be generally less than the model time step but, occasionally, may be greater. This implies that when the solution time is large, the model will fall behind clock time but will catch up when the solution time is small.

Simulations of this type will depend on speed, accuracy, cost of hardware and complexity of the system to be analysed. Models used for energy management systems might have time scales of tens of minutes to several hours, with system states calculated at intervals of one or more seconds [166, 167]. Transient stability studies, on the other hand, will need system states to be evaluated at intervals of the order of tens of milliseconds over time scales of several seconds [168–170].

5.2 Simulations of the British National Grid at the University of Bath

Since the late-1970's, a number of real-time simulations of the National Grid system have been developed at the University of Bath. Hardware and software platforms were generated to allow real-time or faster than real-time simulations to be carried out on single or multiprocessor networks.

Much of the material included here was developed by Dale [168], Berry [169] and Chan [170]. Further additions to this material for mid- and long-term dynamic stability studies involving detailed prime mover and boiler models and voltage dependent loads was introduced by Stagg [171] investigating automatic generation

control. A brief description of the main constituents of the power system simulator (or PowSim) will be given in the next section.

5.3 Power System Modelling

A power network model consists of a loaded transmission system and a set of generators. The general functional block diagram in Figure 5.1 shows the interaction between the models, which will now be described.

5.3.1 Transmission Network

The network is a set of nodes or busbars, teed-circuits or other intermediate points in the system, connected together by branches in the form of transmission lines, cables or transformers.

A single phase network representation is used to model the three phase electrical power transmission network with balanced phase sequence components under steady state conditions. A transmission line or cable is modelled by an equivalent pi-network with half of the total capacitance lumped at each end of the line as an admittance to ground, with the effect of electro-magnetic mutual coupling between double circuit lines ignored. Lines and transformers are lumped together as in Figure 5.2a with transformer taps fixed at their nominal position. Shunt reactors and static capacitors are represented as shunt admittances connected to ground as shown in Figure 5.2b and Figure 5.2c. Busbar loads and fault impedances are modelled as fixed impedances to ground as in Figure 5.3.

5.3.2 Synchronous Machine Representation

The model that has been used is based on Park's transformation of the 3-phase machine into components along the direct and quadratic axis, shown in Figure 5.4. This model only simulates these 3-phase quantities, where damping winding and eddy current effects are represented as a single lumped short circuit winding on each axis shown in Figure 5.5. A set of equations relating the flux linkages can be used to describe the machine, which have been transformed to a voltage behind sub-transient reactance representation to yield easily observable states. The complete derivation of these equations is given in [169, 170].

Air-gap torque equation

$$T_e = E''_d I_d + E''_q I_q - (X''_d - X''_d) I_d I_q$$

Swing equations

$$\begin{aligned} p\omega &= \frac{1}{M}(T_m - T_e - T_{lo}) \\ p\delta &= \omega - 2\pi f_0 \end{aligned}$$

where

$$\begin{aligned} s &= \frac{\omega_o - \omega}{\omega_o} \\ v &= 1 - s \end{aligned}$$

and s is constrained to less than 1 PU and v is assumed to be unity. A number of other approximations are made with $pE'_d = pE'_q = 0$ and for solid round rotor machines $E'_d = 0$, $X_q = X'_q$ and $X''_q = X''_d$.

This results in the industry recommended fifth order model for transient stability studies assuming the machine operates near synchronous speed such that

$$V_d = E_d'' + X_q'' I_q - R_a I_d$$
$$V_q = E_q'' + X_d'' I_d - R_a I_q$$

and

$$pE_d'' = \frac{1}{T_{qo}''}((X_q - X_q'')I_q - E_d'') \quad (5.1)$$
$$pE_q' = \frac{1}{T_{do}'}(V_f - (X_d - X_d')I_d - E_q') \quad (5.2)$$
$$pE_q'' = \frac{1}{T_{do}''}(E_q' - (X_d' - X_d'')I_d - E_q'') \quad (5.3)$$

Figure 5.6 shows the phasor diagram equivalent.

5.3.3 Magnetic Saturation

The saturation factors S_q, S_d are used to model machine saturation and are calculated from the machine open circuit terminal voltage against field current curve as in Figure 5.7. The simulator modifies equations 5.1, 5.2 and 5.3 with assuming that equal saturation occurs at both mutual and leakage paths of the rotor circuits.

This gives the following equations

$$pE_d'' = \frac{1}{T_{qo}''}((X_q - X_q'')I_q - S_q E_d'') \quad (5.4)$$
$$pE_q' = \frac{1}{T_{do}'}(V_f - (X_d - X_d')I_d - S_d E_q') \quad (5.5)$$
$$pE_q'' = \frac{1}{T_{do}''}(KE_q' - (X_d' - X_d'')I_d - S_d E_q'') \quad (5.6)$$

The saturation factor can be defined as

$$K = 1 + \alpha$$

and by introducing new non-integrable variables which are less dependent on the integrable ones, such that

$$\begin{aligned} aE'_q &= \alpha_d E'_q \\ aE''_q &= \alpha_d E''_q \\ aE''_d &= \alpha_q E''_d \end{aligned}$$

Equations 5.4, 5.5 and 5.6 can be re-written in a pseudo-linear form which is more applicable to direct solutions

$$\begin{aligned} pE''_d &= \frac{1}{T''_{qo}}((X_q - X''_q)I_q - E''_d - aE''_d) \\ pE'_q &= \frac{1}{T'_{do}}(V_f - (X_d - X'_d)I_d - E'_q - aE'_q) \\ pE''_q &= \frac{1}{T''_{do}}(E'_q + aE'_q - (X'_d - X''_d)I_d - E''_q - aE''_q) \end{aligned}$$

Similarly, the integrable variables I_d and I_q are replaced by the less dependent non-integrable states V_d and V_q respectively, due to the weaker coupling to E''_d and E''_q.

$$\begin{aligned} I_d &= Y_{re}(E''_d - V_d) - Y''_d(E''_q - V_q) \\ I_q &= Y_{re}(E''_q - V_q) - Y''_q(E''_d - V_d) \end{aligned}$$

where

$$\begin{aligned} Y_{re} &= \frac{R_a}{(R_a \cdot R_a + X''_d \cdot X''_q)} \\ Y''_d &= \frac{-X''_q}{(R_a \cdot R_a + X''_d \cdot X''_q)} \\ Y''_q &= \frac{-X''_d}{(R_a \cdot R_a + X''_d \cdot X''_q)} \end{aligned}$$

5.3.4 Control Systems

To study a power system running either dynamically or transiently after a disturbance, the influences of the machine Automatic Voltage Regulator or AVR and governor systems have been included in PowSim. Several general purpose methods for modelling excitation and mechanical power control that have been published in the IEEE Committee reports [172, 173] have been implemented.

5.3.4.1 Excitation Systems

Dale [168] incorporated a simplified AVR model into PowSim. A stabilising feedback signal was introduced by Berry [169] so that the effects of a high forward path gain could be used without a detrimental reduction in system damping, shown in Figure 5.8. The differential equations used have linear state variables and control inputs, so that

$$pV_f = -\frac{K_g}{T_g}V_s - \frac{1}{T_g}V_f + \frac{K_g}{T_g}V_{err} \tag{5.7}$$

$$pV_s = -\frac{1}{T_s}V_s + \frac{K_s}{T_s}pV_f \tag{5.8}$$

$$V_{err} = V_{ref} - V_t$$

Rearranging and combining equations 5.7 and 5.8 gives a first order equation of the form

$$pV_s = -\left(\frac{T_g + K_s K_g}{T_s T_g}\right) V_s - \frac{K_s}{T_s T_g}V_f + \frac{K_s K_g}{T_s T_g}V_{err}$$

If the stabilising feedback gain K_s is set to zero, the AVR reverts to a simple first order lag.

Chan [170] expanded on this by developing a "composite" model AVR by combining IEEE Type 1 and Type 2 models. This allowed for different AVR types to be selected by altering the settings of the time constants as in Figure 5.9.

5.3.4.2 Speed Governing Model

The governor model implemented by Berry, shown in Figure 5.10, assumes the high pressure cylinder governor valve has an infinite steam source. This valve is controlled by machine speed and steam flow through the high pressure pipework and the reheater are represented by two time constants. This gives

$$\begin{aligned} pV_{pos} &= -\frac{1}{T_a}V_{pos} + \frac{(T_{mo} - K_t\omega}{T_a} \\ pT_{m1} &= \frac{1}{T_b}V_{pos} - \frac{1}{T_b}T_{m1} \\ pT_{m2} &= \frac{1}{T_c}T_{m1} - \frac{1}{T_c}T_{m2} \end{aligned}$$

Chan used the same method with the addition of an interceptor, shown in Figure 5.11.

5.3.5 Simulation Solution Method

To obtain a set of initial conditions to run PowSim, a complex power flow solution is required. This is calculated by National Grid Company's program OPFL02 [174] and given the specified power generation and system loading, initial operating states are obtained by solving the differential-algebraic problem of the form

$$py = \mathcal{F}(y,x) \tag{5.9}$$

$$0 = \mathcal{G}(y,x) \tag{5.10}$$

where y is a vector or integrable variables, such as control system and machine states, x is the vector of non-integrable variables and $\mathcal{F}$ and $\mathcal{G}$ are non-linear vector functions. Equation 5.9 has a pseudo-linear structure that in state space form can be arranged as

$$py = \mathbf{A}y + \mathbf{B}u(y,x)$$

where u is a vector of non-integrable variables, which are some non-linear function of y and x, such that $\mathbf{A}$ and $\mathbf{B}$ are constant matrices. Equation 5.10 can be rewritten in two parts, such that

$$I(E,V) = \mathbf{Y} \cdot V \tag{5.11}$$

and

$$u = u(E,V)$$

where I is a vector of current injections and is calculated from the machine internal voltage E and busbar voltage V for voltage dependent loads if these are present. $\mathbf{Y}$ is the network nodal admittance matrix which is sparse for most large power systems. For a given switching condition, the elements of this matrix are fixed with respect to time.

From this, the main simulation loop is entered :-

1. Calculate the non-integrable variables u_k from the integrable machine and control system states y_k and the integrable voltage states v_k.

2. Calculate the past step quantities c_k (from the integration technique mentioned in [169, 170]).

3. Extrapolate v_{k+1} and u_{k+1}.

4. Calculate y_{k+1} (from the integration technique mentioned in [169, 170]) by forward and backward substitution.

5. Apply limits to the control loop variables.

6. Calculate the machine current injection from E''_q and E''_d.

7. Calculate the busbar injection by summing all machine current injections.

8. Solve the network equation 5.11 to get a better estimate of v_{k+1}.

9. Compare v_{k+1} with the extrapolated value from step 3.

10. If v_{k+1} is converged, advance a time step and go to step 1.

11. Calculate a new estimate of u_{k+1} from v_{k+1} and go back to step 4.

Steps 1 to 6 and 11 are machine group specific and have been implemented as part of a parallel processor version of PowSim by Berry. Steps 7 to 10 deal with the network solution and this has been parallelised by Chan.

5.3.6 User Interface

5.3.6.1 Textual Interface

The initial steady state conditions of the power system model (from OPFL02), together with machine and network parameters, are defined by the user in text files. Most of these parameters can be changed on-line to simulate events such as balanced three phase faults and line outages and can be applied either interactively or as timed sequences of individual events.

Simulator commands can also be stored in files as simple sequences or combined in other commands to create user-defined menus. Each menu can echo some text to the screen and then prompt for a user option, which may then be used to select a number of different command blocks.

5.3.6.2 Graphical Interface

Most of the versions of PowSim that have been developed have supported two displays. A monochrome screen is used to provide textual information (as mentioned above), whilst a colour monitor provides graphics output. The data-logging facility, as developed by Dale and Berry, stores machine and network states for a user-specified duration in memory. These states can then be either transferred to files or plotted to the colour monitor.

In addition to these static screens, animated displays were developed to follow the current state of the simulation, which is continuously updated to run in real-time.

Recently, work has progressed in the area of graphical user interfaces. Ng developed an X-Windows application running on Transputer based hardware [175]. This allows multiple applications to use the same screen and for each application to use several windows. A set of low level graphics routines have been written to provide two display pages with flicker-free dynamic pictures.

5.3.7 Modifications carried out on PowSim

A number of modifications have been made to the simulator program to allow a more realistic view of the power system being modelled

5.3.7.1 Line Protection

A very simple scheme has been added to the simulator code. It uses the principle that if the power through a particular line is greater that its rated MVA, the line is then taken out of the system. This is done by using the relationship : -

$$P = VI\cos\phi$$

There are two modes of operation, namely "manual" and "auto". The latter is for protection to be included in the simulation, the former to exclude it to allow the user to outage lines manually with no interference by the protection module.

However, whilst running the simulator after a large system disturbance, it became evident that this protection scheme was too simplistic. The problem that arose was a line could trip out and be reconnected an infinite number of times, which is naturally an inaccurate model to use.

Therefore, a more realistic system has been implemented, which uses a similar principle to that of modern day "DAR" (Delayed Auto Reclose) protection schemes. Hence, once a line has been tripped and reclosed twice (after 200ms), the next event that it is outaged leaves it permanently disconnected from the network.

5.3.7.2 Addition of Acceleration Feedback Signal to the AVR Model

Calculations of kinetic energy and rotor acceleration have been added to the machine code within PowSim to allow the addition of a further stabilising feedback signal to the generator excitation system. The equations used are

$$Ke = \frac{1}{2}(M\omega^2) \tag{5.12}$$

and

$$Acc = \frac{1}{M}((T_{m1}K_1) + (T_{m2}K_2)) \tag{5.13}$$

These are calculated along with the machine equations every time step and are used for transient stability assessment and braking resistors.

5.3.7.3 Braking Resistors

The practice of installing braking resistors on generator terminals has been introduced to PowSim. However, the principle of adding a resistor of Megawatt capability to ground was found not to be suitable and, instead, various methods were devised to simulate the same effect. The final decision was to connect a load to the generator busbar which directly mimic the generator output. The signal used to switch this load on to the generator terminals was eliminated down to two inputs, namely that of machine kinetic energy and rotor acceleration from equations 5.12 and 5.13 above. The former was found to be less accurate than the latter. Hence, an acceleration signal is used, which, when above a suitable limit, switches the load in but takes the load off the busbar when the rotor has slowed down, again between specified limits.

5.3.7.4 Area Recognition

An additional element has been added to the power system components, such as lines, busbars and generator groups, by specifying a geographical area in which they are located. This is of principle use in alarm processing, where it was thought that an alarm warning would be more easily identified by an operator than the present system set up allows.

5.4 Summary

The power system models and techniques that were used in the real-time simulator PowSim have been described. Many developments have matured during its evolution from six MC6800 microprocessors (Dale) to twelve processors (Berry) enabling an increase in power network study size from four generators and six busbars to twenty machines and sixty nodes. Final extensions to this by Chan allow an eighty machine and eight hundred node system to be run in real-time making use of sixteen INMOS T800 transputers via parallel processing techniques. Work has also progressed into providing an enhanced user interface.

Serial versions of the simulator have been ported to run on other hardware such as PCs, SUN and APOLLO workstations and an Intel i860 processor plug-in board hosted by a PC.

Extensions have been added to the basic PowSim model in preparation for the main thrust of the security assessment algorithms which will be described in Chapter 7. A serial version of the simulator running on an i860-based PC will be used together with the latest addition to the available computer hardware, a Silicon Graphics Indigo R4000. The hardware and associated operating systems will be outlined in the next chapter.

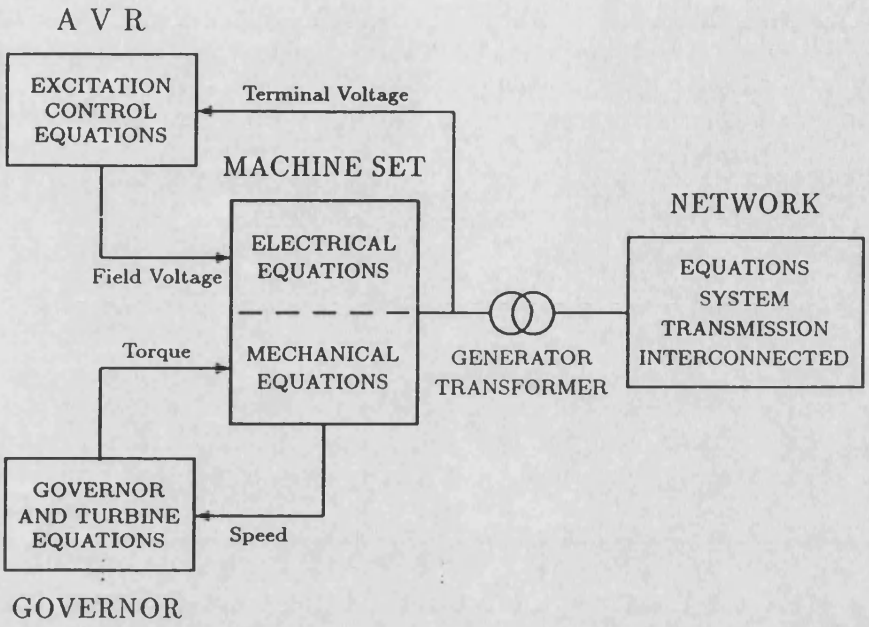
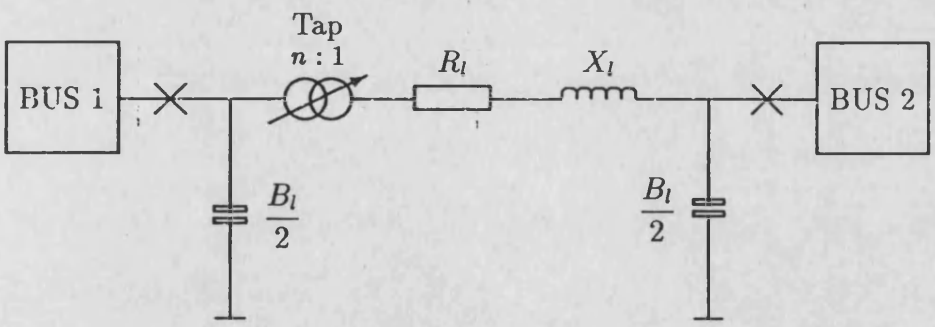
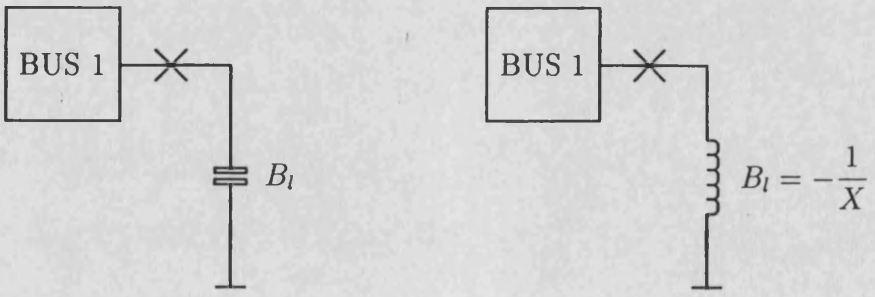


Figure 5.1: Model Structure



a) General line or transformer



b) Capacitive shunt

c) Inductive shunt

Figure 5.2: Network Branch Equivalent Circuits

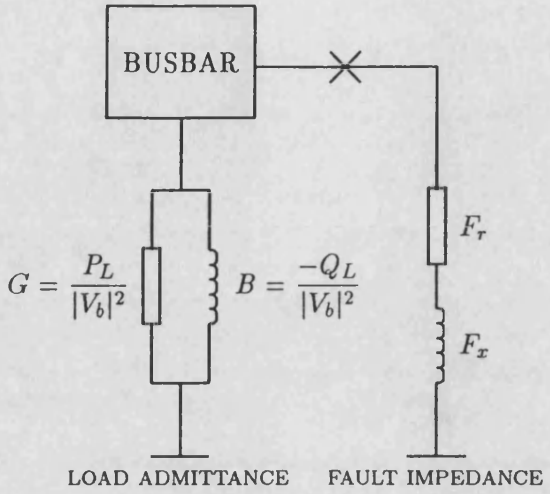


Figure 5.3: Busbar Load Model

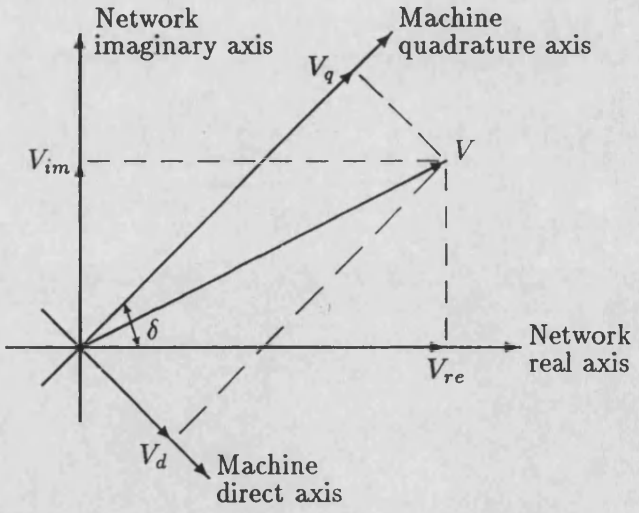


Figure 5.4: Synchronous Machine and Network Frames of Reference

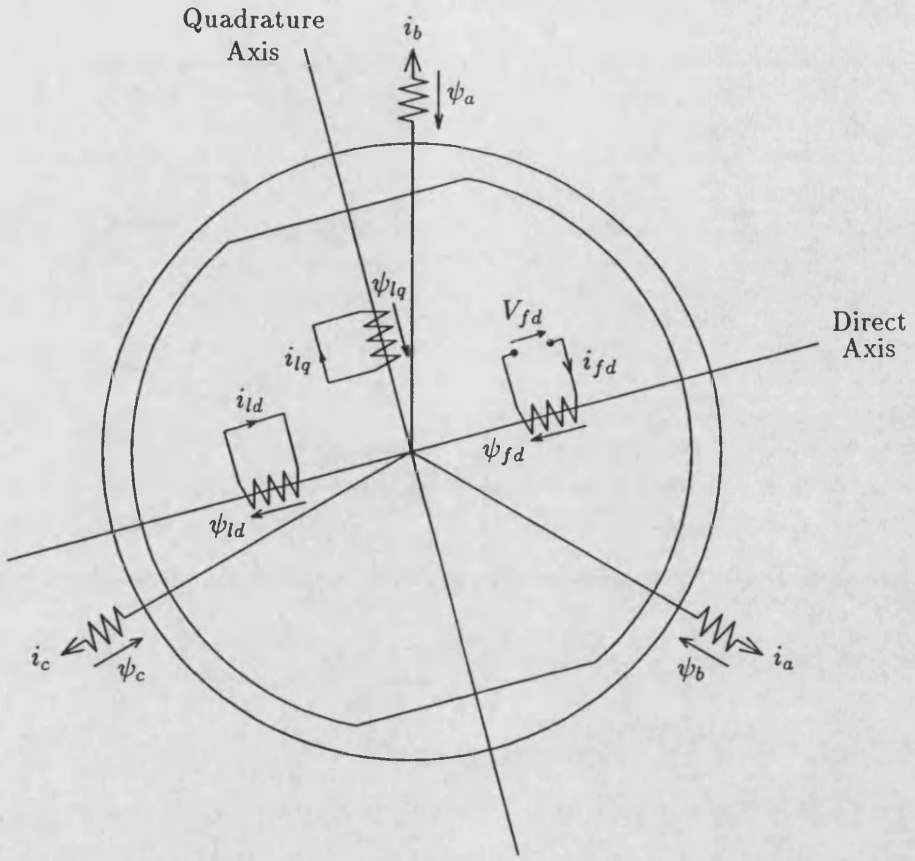


Figure 5.5: Synchronous Machine Winding Arrangement

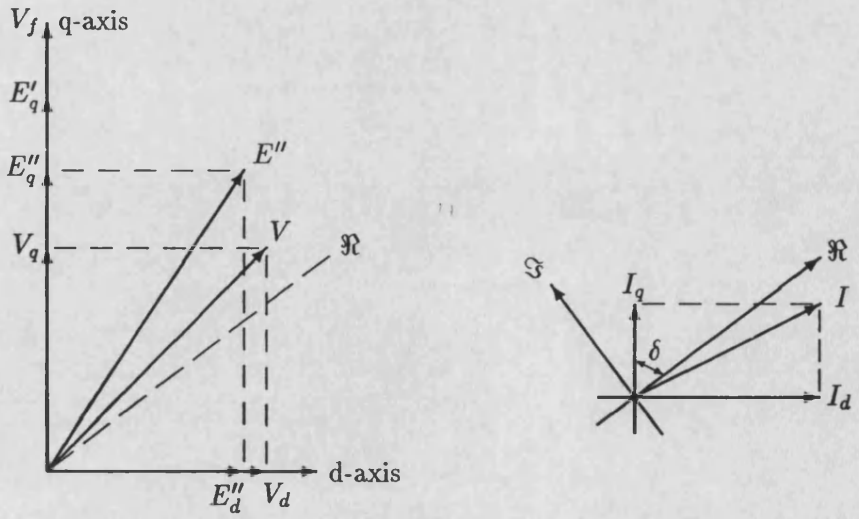


Figure 5.6: Phasor Diagram for Subtransient Condition

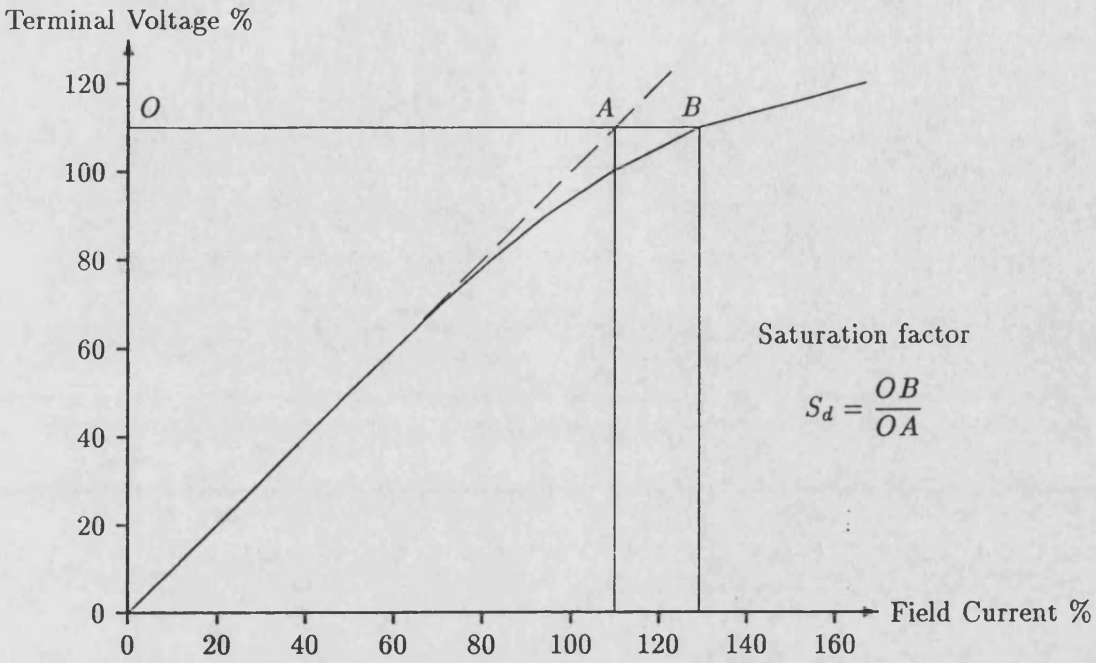


Figure 5.7: Generator Open Circuit Saturation Characteristic

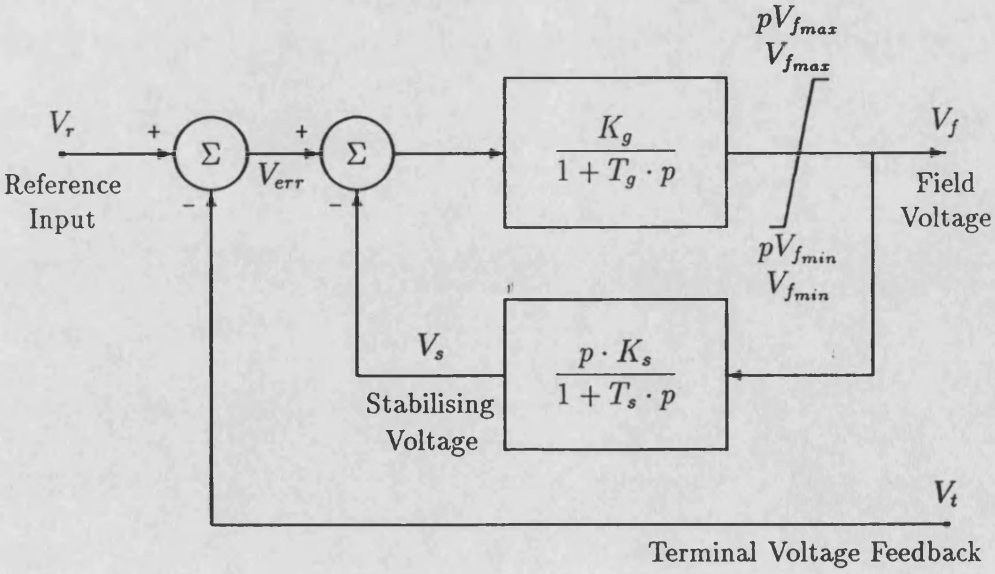


Figure 5.8: PowSim AVR Model

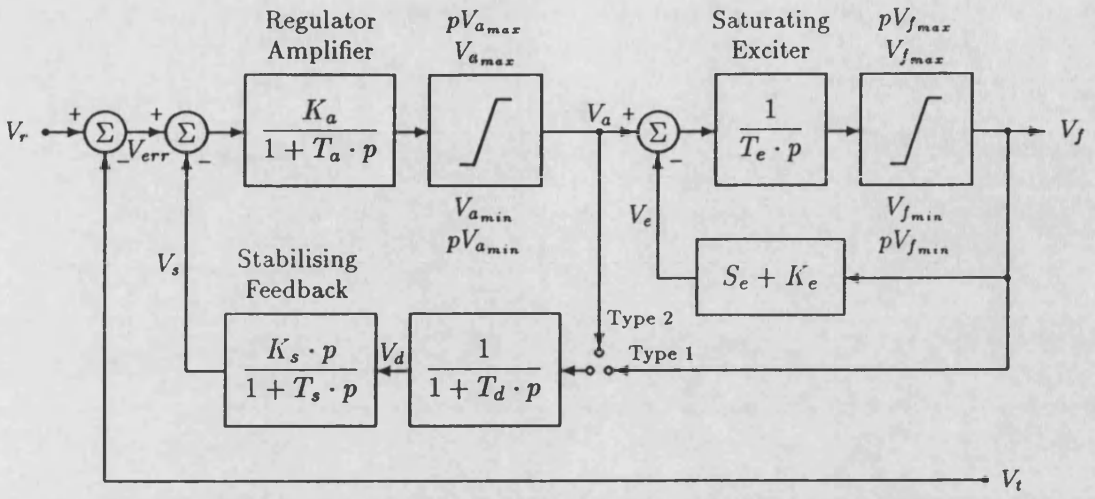


Figure 5.9: Simplified Composite IEEE AVR Model

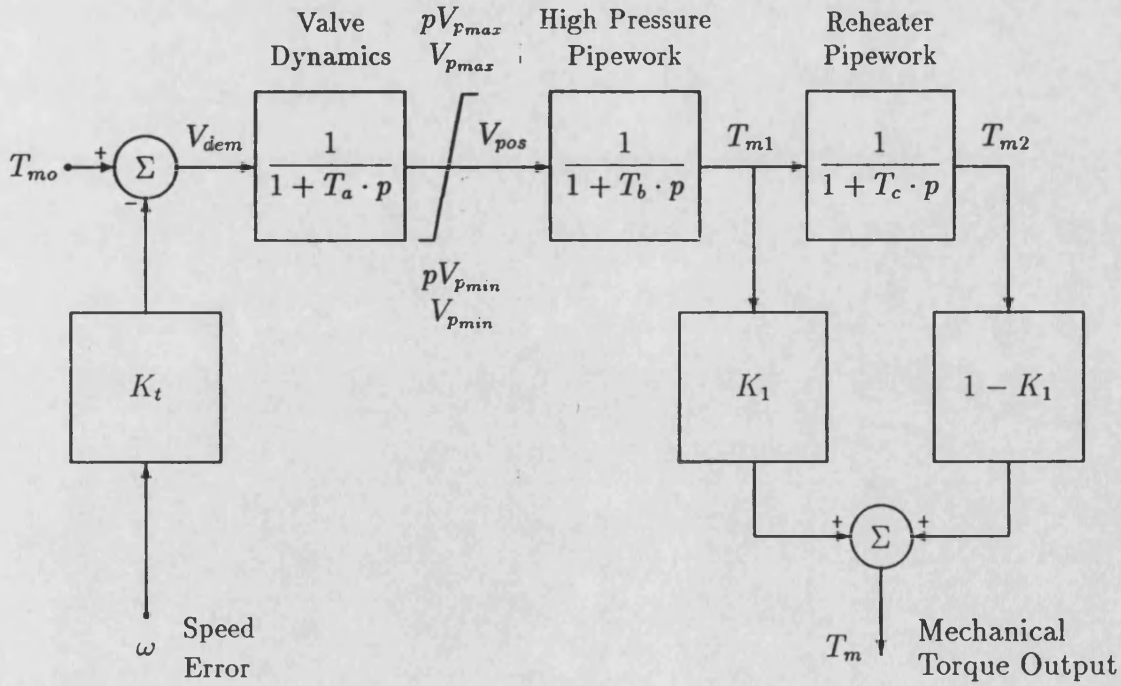


Figure 5.10: PowSim Speed Governor and Valves Model

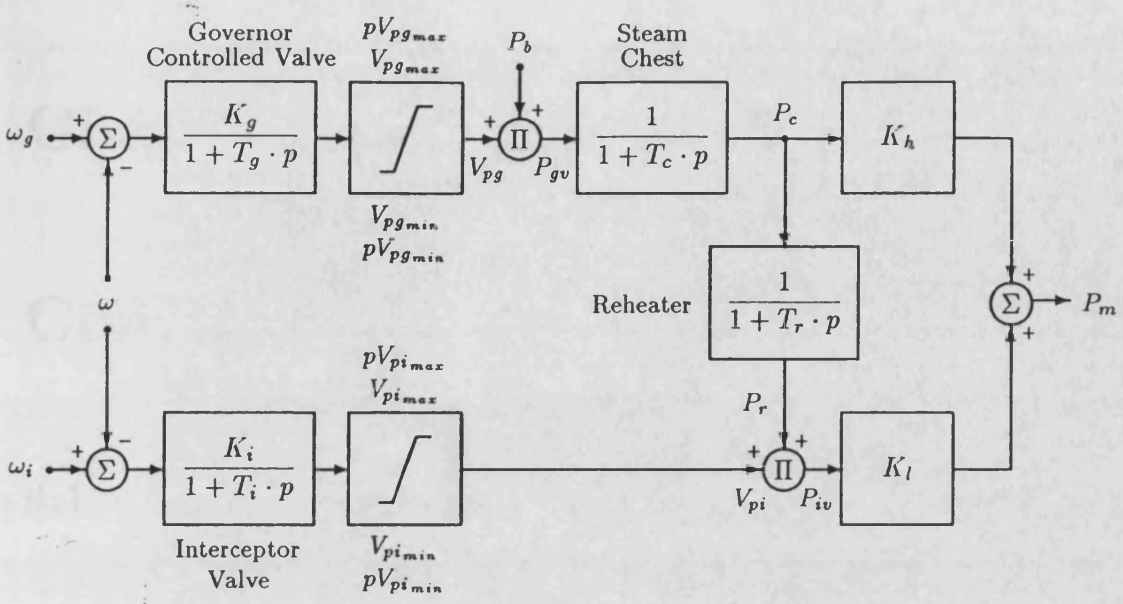


Figure 5.11: Speed Governor and Valves Model Including Interceptor

Chapter 6

Computing Hardware

6.1 Introduction

The power system simulator described in the previous chapter has been ported to a number of hardware platforms for both serial and parallel architectures. In this research, a serial or single processor version has been used to run PowSim and security assessment software on a Microway Number Smasher-860 hosted by a personal computer (PC) and a Silicon Graphics INDIGO. A mention will also be made of how the latter architecture has been used in a distributed parallel processing approach for an on-going research programme.

Each hardware base and its associated operating system, will be described in the following sections. More emphasis is placed on the Number Smasher-860, since the majority of the development was been carried out on this architecture.

6.2 Microway Number Smasher-860

6.2.1 Board Specifications

Microway's *Number Smasher-860*, NS-860, [176, 177] is an accelerator card that can provide personal computers with supercomputer throughput at microcom-

puter prices. The board is powered by a 40 MHz Intel 80860XR or *i860* microprocessor with 32 megabytes of 64-bit four-way interleaved dynamic RAM (DRAM) and is hardware compatible with both ISA and EISA architecture in any existing IBM PC/AT 80286, 80386 or 80486 acting as the host. In this research, a math co-processor equipped 33 MHz IBM PC/AT-386 clone with 4 megabytes of DRAM running the MS-DOS (Version 5.0) operating system has been used as the host for the NS-860 board. This combination has been shown to run three to ten times faster than the standard 386 system using the Whetstone benchmark. The PC is equipped with a colour VGA monitor and a mono monitor in order to operate in a two-screen mode, the former for graphics and the latter for interactive user textual input.

The NS-860 delivers up to 80 million single precision floating point operations per second at 40 MHz and produces 12 double precision Linpack megaflops as compared to the standard 386 system which typically produces between 0.2 and 1.4 Linpack megaflops. Hand-coded versions of the dot product routines, SDOT and DDOT, process 20 and 40 million multiply accumulate pairs per second in conditions when one of the vectors is in the i860's data cache. The Intel claim of 40 to 80 million operations per second is based on these hand-coded dot product routines.

The number smasher includes an AT link adaptor interface that allows the board to communicate with the host 386 over its ISA bus. The transfer rate of these link adaptors on the board used for this research was 0.8 megabytes per second, although an ISA FIFO interface has been developed by Microway to take advantage of the full throughput of the bus and increases the data transfer rate to 2.5 megabytes per second. The EISA FIFO interface allows the parallel operation of several NS-860 cards and achieves throughput rates that approach 33 megabytes

per second transfer rate.

The board includes a boot EPROM which contains power-on code and a monitor which initialises the i860 and supports communications with the 386 host via the two built-in link adaptors and the ISA bus.

6.2.2 Advantages of a Standalone Board

The NS-860 offers several advantages over i860 cards that share memory with their host :

- Memory interface design : the 386 and i860 each achieve peak performance using different memory management strategies. The memory design that is optimal for the i860's interleaved memory is not necessarily optimal for the 386 bus.
- Neither the i860 nor the 386 can deliver peak performance operating under a shared memory environment which must serve between the two processors as well as using the non-optimal memory interfaces. This becomes apparent and, in some cases, severe when the 386 manages I/O while the i860 simultaneously loads bytes from memory every other cycle.
- The flexible interface of the NS-860 boards makes it ideal for either standalone, as is the case for this research, or for massively parallel problems and can be run in any existing micro PC system without the need to buy a new motherboard.

6.2.3 Compiler Structure

The *NDP-860* compilers incorporate a Common Object File Format or COFF based tool set, an i860 assembler, linker, librarian and loader which run under MS-DOS, the PC's operating system, and contain a library of device-independent graphics routines with enhanced features that support VGA and Hercules adaptors.

The compiler is distributed as a native compiler which consists of i860 binaries that are loaded from an 80×86, but execute on the i860 resulting in enhanced compilation speed. Code can be interfaced with assembly language and between Fortran, C, C++and Pascal NDP compilers, since they use the same calling conventions for procedures.

The NDP-860 compilers run on Microway's *XTEND-860* environment [178], which is similar to an alien file server developed for the transputers that Microway have marketed. It is composed of two parts : *RUN860*, an alien file server that resides on the 386 host and *OS860*, a protected mode supervisor that resides on and manages the i860.

6.2.3.1 RUN860

RUN860 is a C application that runs on 286, 386 or 486 platforms under MS-DOS. Two versions exist : *RUN860.EXE* which is a real mode loader and *RUN860P.EXE* which is a protected mode loader used for graphics applications, using the Microway *GREX* library.

Both variants use device drivers to control I/O between the NS-860 board and the

386 host and contain features which help in debugging and timing code. As an example, the -v or "verbose" switch prints out the addresses used to load OS860 and the application, as well as the time spent in various parts of the load/run process. A complete lower level debugger is also contained in both versions that enables the user to print and use symbolic information, debug pipelined code and display and work with numerical data in memory, registers or the pipeline using conventional floating point formats.

Microway is currently undergoing a development program to create interfaces between the i860 and the real and the protected mode devices needed to simplify the ports of some DOS-based products.

6.2.3.2 OS860

The OS860 kernel is loaded into low memory by RUN860 and performs the following tasks :

1. Boots itself from the 386 host.
2. Sets up the paging tables needed to manage memory.
3. Installs a general purpose exception handler.
4. Loads and runs applications.
5. Handles communications with the host including :
   (a) i860 exception messages including :
      i. numeric exceptions
      ii. page faults

(b) 386 based debugger requests for information on

i. register and memory contents.

ii. the setting of traps for break points and single stepping.

(c) Runtime communications between the 386 and the i860 runtime system using traps to the kernel that manage the 386-i860 communications.

6. Manages the applications memory space making it possible to implement protection between tasks and the kernel in addition to providing a consistent mechanism for allocating memory.

7. Provided a user interface to the numeric exception handler.

6.2.3.3 NDP C/C++-860 Compiler

The power system simulator PowSim and all code developed during the period of this research has been written in the C programming language so that the *NDP C/ C++-860* compiler could be used. This supports Kernighan and Ritchie C, Ansi C and the AT&T Version 2.1 C++specifications in a UNIX-like environment (BSD 4.2 and AT&T Version 3).

The compiler also includes an on-line assembly language interface that simplifies the development of embedded code, device and screen drivers and operating systems by allowing the programmer to specify register values and generate interrupts. This facility can permit the programmer to subsequently design software in an *Object-Oriented* approach.

The compilation process involves compiling, assembling, linking and running a program. After compiling, the assembler creates an object file with extensions

of the form .o directly from the assembly code. The linker takes the object file together with other specified files and libraries and produces a NS-860 specific executable.

In order to compile the power system simulator to facilitate animated displays, the NS-860 executable is linked with a Microsoft graphics routine to provide graphics and I/O extensions for the i860. This results in an executable that can be run from the 386 host on the NS-860 board.

6.3 Silicon Graphics INDIGO

6.3.1 Hardware Specifications

The INDIGO [179] is a culmination of many computing technologies that have been developed over a number of years by Silicon Graphics. It is based on the product of the third generation MIPS RISC architecture built around a R4000 processor running at 100 MHz offering 85 MIPS, 16 MFlops and 70 SPEC 89 marks performance. The CPU and memory bus can achieve 400 MB/sec with a throughput from the 64-bit system I/O bus of 267 MB/sec. The INDIGO, in addition to its 16 KBytes of primary cache (8 KBytes each of data and instruction cache), also has a 1 MB secondary cache, which enables very fast performance by providing the largest cache on a desktop workstation at the time of writing.

The architecture itself allows a huge memory expansion (up to 384 MB RAM), although, only 32 MB of main memory are supported in this set-up. Four industry standard EISA slots (or two EISA slots with high performance GIO-64 slots) are also available for further hardware expansion. The 1.2 gigabyte hard disk and peripheral configurations to external PCs are accommodated by a fast independ-

ent SCSI-2 controller and an integral 10 Base T Ethernet connection. Together with two serial RS422 (38.4K baud) ports, a bidirectional parallel port and five audio I/O connections, this set-up, therefore, makes the INDIGO suitable for both standalone functions and a networked environment.

X Windows and 2D graphics are supported by the INDIGO's graphics card. This also supports 3D image processing through a software Z buffer and host-based geometry calculations. The REX3 Raster Engine ASIC converts geometric data processed by the CPU into pixel and line data that it then writes into the frame buffer. This is supported by a 17" monitor with 1024 $\times$ 768 resolution, 4096 colours and a 76 Hz screen refresh rate. This enables a pixel fill rate of up to 437 million pixels and 1.4 million X Window (X11) lines per second. Additional standard graphics features include texture mapping, depth cueing, stereo graphics and pan and zoom facilities.

6.3.2 The UNIX Operating System

Underlying any applications or tools that can be used on the INDIGO is the *Irix* operating system (Version 4.0.5F) which is an adaption of the well known *UNIX* operating system [180]. Irix is much more flexible and powerful than traditional personal computer operating systems, such as MS-DOS, highlighting a number of features which are inherited from the basic UNIX :

- It is a multi-user operating system, which means several users can work on the system simultaneously and maintain private files.
- The INDIGO is made into a multi-tasking system, permitting the INDIGO to run several applications, print files and update files at the same time.

- The INDIGO can be connected to a network, where files can be transferred to and from another workstation, in this case, via the ethernet connections to a number of peripheral PCs.
- Irix allows a number of hardware bases to be added such as printers, terminals and disk drives without the need for additional software.

6.3.2.1 Basic UNIX Structure

The operating system, often referred to as the *system kernel* interacts directly with the INDIGO hardware, providing common services to programs and "insulating" them from any hardware quirks. In this way, programs become independent of the hardware base and can be easily moved between UNIX systems running on different architectures.

The kernel performs various operations on behalf of those processes that are used to support the user interface. These services provided by the kernel may control the execution of processes by allowing their creation, termination or suspension, as well as communication between them. Secondly the execution of these processes can be scheduled fairly on the CPU, i.e. in a time-shared manner, by executing a process and suspending it (if its operation time has elapsed), scheduling the next process and later returning to any previously suspended actions.

The kernel also allows processes to share portions of the main memory during program execution. If the system runs low on memory, the kernel frees memory by writing a process temporarily to disk secondary memory, which is called a *swap device.* This secondary memory can be allocated by the kernel for efficient storage and subsequent retrieval of user data and, hence, in this function, it constitutes a

file system. The kernel can allocate secondary storage for user files, reclaim unused storage, structures the file system and protects user files from illegal access.

Finally, the kernel provides these services "transparently". It supports the services, for example, that the "shell" needs to act as a command line interpreter by allowing the shell to read terminal input, synchronise process execution and redirect I/O.

6.3.3 X Windows

The *X Window system* [181], or *X* as it is often referred to, is a network-based graphics windowing system that was developed by Massachusetts Institution of Technology in 1984. Several versions of X have been developed, the most recent of which is version 11 (*X11*), first released in 1987 and it is this that is used on the INDIGO.

The X system architecture can be split into two main components : *display servers*, which provide display functions and keep track of user input and, *clients*, which are application programs that perform specific tasks. This partition allows clients and display servers to either work together on the same system or be separated over a network running on isolated machines.

6.3.3.1 X Display Server

The X display server is a program that keeps track of all inputs coming from the keyboard or mouse or from any other clients that are concurrently running. As the display server receives data from a client, it updates the appropriate window on the display and may run on the same computer as a client or an entirely different machine.

6.3.3.2 Clients

X allows a number of clients to be run at the same time. Even though these programs may display their results and take input from a single display server, they may each be running on a different computer on the network. Other examples of client programs used on the INDIGO include :

- *4Dwm*, the Silicon Graphics window manager. This allows windows to be moved around the screen, as well as changing the size of these windows. Windows can also be raised or lowered (brought in front of others or sent behind them, respectively) and converted to icons or vice versa within 4Dwm. Another important feature of the window manager is to create additional shell windows.
- *winterm*, the Silicon Graphics equivalent to the X11 *xterm*, which provides a terminal emulation within a window. Anything that can be done on a standard terminal (such as a DEC VT102 or Tektronix 4015) can be conducted in this shell window and can be used to run other clients. This has many additional features, compared to a traditional terminal, which include scrollbars and a copy and paste facility between windows.

In order to run PowSim, two windows are created : a graphics display and a text window which are equivalent to the colour and mono monitor respectively as for the PC-based version

6.4 Distributed Parallel Processing Architecture

A research programme, cofunded by SERC and National Grid Company, was set up in mid-1992 to investigate and develop a dynamic security assessor for on-line use in a grid control room [182].

Even for a medium sized power network, the required computational power would exceed the limit for real-time operation in typically a 10-15 minute time interval. It was suggested that a fair amount of parallelism exists among the assessment modules, described in Chapters 2 and 3 of this thesis, so that the use of distributed processing became a practical solution.

6.4.1 System Software and Hardware

The preliminary computer system hardware used for the "On-Line Algorithm for System Instability Studies" or OASIS consists of the Silicon Graphics INDIGO, a number of IBM PC/AT compatible 80386 and 80486 computers and a DEC ALPHA Series 3600. Figure 6.1 shows how these components are networked together with ethernet connections in a heterogeneous computing system.

In this configuration, the INDIGO workstation works as a *network server* for the rest of the system, with a local disc exported as the network drive via the *network filing system, NFS.* An additional ethernet card has been recently installed so that the local ethernet can be isolated from the main university network.

All IBM PC/AT compatible 386 and 486 computers are identical with 8 megabytes of memory, ethernet card, math co-processor and dual monitors. Local processing power is boosted by either an i860 or T800 accelerator card. A dual operating

system is used consisting of MS-DOS version 5.0 and Linux. The latter is a freely available UNIX compatible operating system with complete networking and X Windows facilities for developing the graphics interface for OASIS.

The ALPHA workstation has been recently acquired and, in this network setup, is used in a similar way to the PCs, i.e. where jobs are allocated to it in a parallel tasking manner. It, however, like the INDIGO, has superior processing power over the IBM PC/AT compatibles.

6.4.2 OASIS Software Architecture

The software architecture of OASIS is founded on the use of Open Systems standards or POSIX. ANSI C and C++are used as the principle programming languages to ensure the portability for all major pieces of code, with UNIX compatibility maintained for all of the computing subsystems mentioned above.

As mentioned in previous chapters, a complete dynamic security assessment system comprises of a number of functional blocks which can be sub-divided into a set of co-operating processes running on a distributed or multitasking system as in Figure 6.2. Interfaces between these modules have been designed so that each block can operate independently with I/O redirected to the common database system.

A software *backplane* based on Oak National Laboratory's Parallel Virtual Machine (PVM) has been built over the individual computer architectures so that the network can work as a single virtual machine. PVM is composed of a daemon and a library of interface routines and supplies functions to automatically start up processes on the virtual machine and allow these to communicate and synchronise

with each other.

6.5 Chapter Summary

This chapter has described the hardware facilities and programming and operating system environments used for the development and testing of the security assessor as part of the power system simulator PowSim.

The majority of the development work was performed on a Microway Number Smasher-860 hosted by a IBM PC/AT-386. Testing of the algorithm modules was carried out using this architecture and a Silicon Graphics INDIGO.

An additional computing system, that of a heterogeneous network, has been briefly described, which was set up for a further research programme into the area of dynamic security assessment and illustrates how system analysis could be carried out over a distributed computer network.

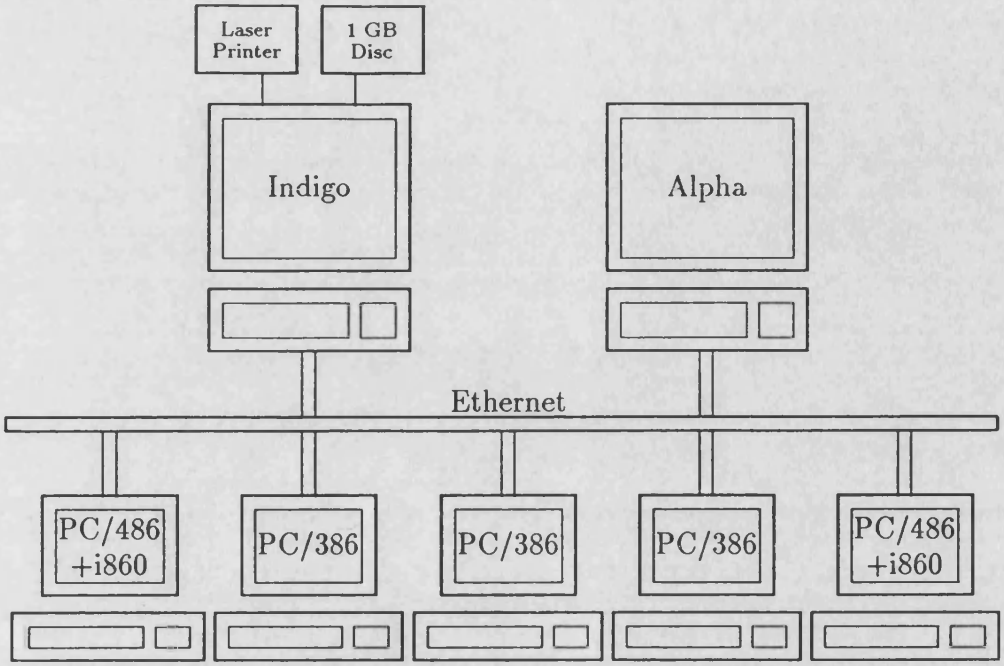


Figure 6.1: Security Assessment Hardware Structure

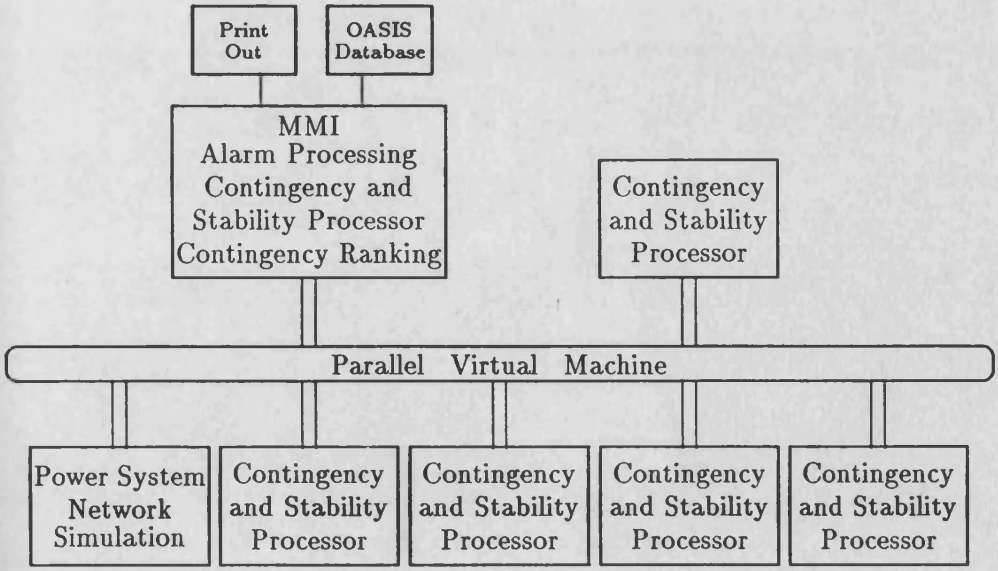


Figure 6.2: Security Assessment Software Structure

Chapter 7

Software Implementation

7.1 Introduction

The power system simulator PowSim described in Chapter 5 of this thesis has been used as the basis for the dynamic security assessor. All computing code was written in ANSI standard C programming language [183–185], so, in order to retain compatibility and portability between different hardware platforms, the system analysis software was also written in this language.

In keeping with how this thesis has been structured, the security assessor implementation was split into three distinct divisions namely, contingency analysis, stability assessment and alarm processing. Each division will now be explained in the following sections.

7.2 Contingency Analysis

As mentioned in Section 5.3.6, PowSim has been developed to include a textual or interactive interface between man and machine and allows a number of parameters to be changed on-line by the user, which include : -

- Switch busbar faults on or off.

- Switch transmission lines in or out of service.
- List or change busbar loads.
- List or change line impedances and/or transformer tap ratios.
- List or change generator group power output and group disconnections.
- List or change generator set transformer tap ratios.
- List or change AVR parameters and set points.
- List or change governor parameters and set points.

A data logging facility is also available which stores machine and network states for a user-specified duration in memory and can be either transferred to files under user control or plotted to the colour monitor or window immediately (depending on which computing platform is being used).

7.2.1 Overview of Main Loop

The source code that allows this interaction was used as the basis for applying contingencies, i.e. busbar faults, line outages, etc ... The operations listed in Section 7.2 above are split into "command modules" which are called by the user via the man-machine interface to carry out the modifications to the operating point of the simulator. An additional module has been written called "`Cmd_Contg`" which reads all the credible disturbances in a user-specified database and calls the appropriate routines to conduct contingency application and analysis. The procedure involved is summarised by Figure 7.1.

The database contains single and multiple circuit transmission line outages, busbar faults, load losses and generator trips and the user specified time periods for

contingency screening, analysis and any further stability assessment that may be required for dynamic instability cases. Fault duration for busbar contingencies are also specified in this database.

For each contingency read in by `Cmd_Contg`, a check is carried out by the code to see whether it is a valid proposal, i.e. if a particular busbar specified in the database is in fact in the network model. If it passes this check, all performance indices and network/stability alarm flags are set to initial nominal values in the relevant contingency structures before the contingency is applied. In the particular case of line outages, a local or remote end flag is also set to specify which end of the transmission line is to be tripped first. If a contingency contains the keyword "and" in the database, a multiple outage has been specified.

Before any contingencies are applied, the pre-contingent system state is remembered, so that the network can be restored to its original operating condition at the end of each contingency analysis period. The outages listed in the database can then be passed to the application code, the data transferred includes contingency type and name together with the screening, analysis, fault duration and dynamic stability assessment time periods specified in the database.

7.2.2 Application Routines

From the main loop in Figure 7.1, the appropriate function calls are made to the relevant *Contingency Application Routines.* If the example of a line outage is used, it can be seen from Figure 7.2 that there are a number of objects passed to the function. Alarm logging for both network and transient stability violations (which will be described in a later section of this chapter) and contingency screening are started simultaneously and call routines from the main simulator loop which

invokes the network and machine calculations discussed in Section 5.3.5. The SCREEN flag is set to TRUE whilst the simulator is screening the contingencies for subsequent processing. The time period for this screening interval is specified by the user in the database and for this research it was found that 1 second proved to be adequate.

During this interval, the fuzzy *Contingency Analysis Routines* are called and starts processing the data coming from the simulator immediately after the fault has been applied. Thesewill continue in their operation until terminated by the contingency.

In the case of line contingencies, in addition to the line name (or names, for multiple outages), the side which is to have primary tripping is also passed. In early studies, lines were simply taken out of service, which, although this was acceptable initially, consultation with National Grid Company revealed that a more accurate line contingency application was needed. The local end busbar of the line is tripped with a 3-phase fault of 80ms duration and the fault impedance to ground from that busbar is set to zero, i.e. disconnecting the line from that busbar. The remote end is tripped at the same time as the sending end but with a longer 120ms 3-phase fault and a fault impedance to ground equivalent to the impedance of that line, i.e. the remote end still "sees" the line in service. Once the fault at the remote end has been cleared (40ms after the sending end), the line is completely removed from the network. This is an example of a single line contingency with the local end tripped first. The procedure is similar for primary remote end tripping and can be easily adapted for multiple circuit outages.

This procedure is similar for other types of contingency, i.e.

- Busbar faults; the analysis is carried out once the busbar has been subjected

to a 3-phase fault of duration specified in the database.

- Busbar load losses; the pre-contingent busbar load is stored and set to zero during the contingency application whilst analysis is being carried out.
- Generator group trips; the generator is tripped or disconnected from the rest of the system during the contingency analysis period.

If after the screening interval, i.e. when the screening period has elapsed and the SCREEN flag is set to FALSE, no network violations have been received by the alarm processor, this contingency is deemed to be not harmful to the system and no further analysis takes place. A similar logic is used for transiently unstable situations. However, since this is a worst case scenario, it is given a maximum rating by the contingency analysis software and stored with its associated network and stability violations for subsequent ranking.

If any contingencies pass through this first filter, the ANALYSIS flag is set to TRUE, which is similar in its effect to the screening operation by calling the transient stability assessment code, as well as alarm handling and contingency analysis routines. However, this time it also calls a dynamic/steady state stability analysis algorithm. Again, if any transient instability is detected during this period, further analysis of the contingency is stopped. When this analysis time has elapsed, which is again specified by the user in the contingency database (for this research a 10 second interval was used), all performance index calculations are terminated, i.e. the ANALYSIS flag is set to FALSE.

An additional time period for dynamic stability analysis is utilised only when the magnitude of power oscillations in the network exceeds a threshold value. This will be described in more detail in a later section. If during this time, these oscillations

die out or are below the specified level, any further stability analysis is stopped.

The line, busbar/load or generator is then put back into service and the power system is restored to its original pre-contingent operating condition ready for the next contingency with all of its performance indices and alarms stored in memory for subsequent ordering and presentation of the final results.

7.3 Analysis Algorithm

During both the screening and further analysis periods discussed above, the degree of severity of the contingency and its impact on the system is measured. The approach used is based on fuzzy-set theory as described in Chapter 4 of this thesis. Four contingent quantities are monitored : -

1. Line power flows in MVA.
2. Busbar voltage magnitudes in p.u.
3. Generator group power outputs in MVA.
4. Reactive power injections in MVAr.

Figure 7.3 outlines the basic procedure. Each quantity is normalised with respect to its operating limits, i.e.

1. for each line, $x_l = \frac{MVA_{flow}}{MVA_{rated}}$.
2. for each busbar[1], $x_v = \frac{(V_{mag} - 1.0)}{0.05}$

[1]This is based around a Wasley and Daneshdoost algorithm [62] and is modified by Ekwue [69] for National Grid Company voltage directives, i.e. a 5% change

3. for each group, $x_g = \frac{MVA_{gen}}{MVA_{rated}}$

4. for each group MVAr injection, $x_q = \frac{MVAr_{inj}}{MVAr_{limit}}$

where x_l, x_v, x_g and x_q are the normalised line MVA flow, busbar voltage magnitude, group MVA power output and group MVAr injections respectively.

Each normalised quantity is divided into five categories by fuzzy set notation. Experiments using three or ten divisions show that, for the former, less accuracy but greater computational speed can be achieved. For the latter, on the other hand, the accuracy was comparable to using half the number of categories (but with more computational overhead) and, hence, five classifications have been used. These categories are principally *Very Small* (*VS*), *Small* (*S*), *Medium* (*M*), *Large* (*L*) and *Very Large* (*VL*). The relationship between these fuzzy linguistic variables and the normalised quantities needs to be defined. As an example, for the case of busbar voltage magnitudes, those normalised deviations from the nominal 1.0 p.u. that are of the order of 0.1 or 0.2 (equivalent to a 1% step change) may be classified in the *Very Small* category, whereas those that have deviations of more than 0.6 (or 5% change) are deemed to be *Large* or even Very Large.

The membership functions μ of these linguistic variables have been represented by triangles, which have been used for computational speed as compared to the more commonly used polygon approach, with no decrease in accuracy. The triangular membership function can, therefore, be described by its centre (*C*), width (*W*) and peak (*P*). As discussed by Hsu et al. [41], the definitions of these are : -

- The centre of each triangle gives a measure of the most possible or likely relative severity for each linguistic variable, so that for a plot of membership

function against system performance index (PI) for a particular contingent quantity, as in Figure 7.4, it can be seen that the *VS* linguistic variable has a lower PI than that for the *VL* category, for severely violated conditions.

- The width of each triangle represents the degree of uncertainty about the performance index. As in Figure 7.4, the *Medium* linguistic variable has a greater uncertainty compared to *Very Small* or *Very Large*. This is typical of a humanistic view of line flows. For example, an operator may say that 20% loading of a transmission line is *Very Small* and 120 % is *Very Large*, but he/she cannot precisely define what the limits are for the *Medium* range, other than to say "somewhere in between".

- The peak value gives the measure of the relative strength of the linguistic variable. It can be seen in Figure 7.4, the variables have been initially weighted by a "sigmoid function" so that more emphasis can be placed on the *Medium* to *Very Large* range, since this is ultimately of greater interest than the region below this in performance index terms.

Various other weighting functions for the initial peak values of the triangles have been used such as a constant approach ($\mu = 1$ for all linguistic variables), a linear $\mu \equiv PI$ method and an exponential curve. These are described in Table 7.1 and Figures 7.6, 7.7 and 7.8. Results from each of these will be discussed in the next chapter.

The relative severity of each contingent quantity, as it is calculated by the main simulator loop, is evaluated from its normalised value and the classification triangle parameters into which it falls, so that for the *Small* linguistic variable describing busbar voltage magnitude

$$PI_S = \left((C_S - W_S) + \left(\frac{x_v - 0.2}{0.3 - 0.2} \times 2W_S\right)\right) \tag{7.1}$$

where C_S and W_S are the centre and width of the *Small* triangle respectively and 0.2 and 0.3 are the lower and upper normalised deviation ranges for that variable. From this the membership function for this example can be calculated so that

$$\mu_S = \left(P_S - \left(P_S \times \frac{PI_S - C_S}{W_S}\right)\right) \tag{7.2}$$

where P_S is the initial peak value of the membership function triangle. If a number of contingent quantities fall into a particular linguistic variable, the membership function of that variable is modified or enhanced by the use of fuzzy-set notation operations, i.e. the peak value of the triangle increases illustrating the dominance of that linguistic variable. For example, for a post-contingent condition, the shape of Figure 7.4 can resemble something similar to that of Figure 7.5 if more *Small* violations are present compared to say *Large* or *Very Large*.

From Figure 7.5, it is not apparent what the total system performance index is for this particular contingent quantity. In order to calculate this, a process known as "defuzzification" is used. There are two main methods for achieving this, namely *max-min* and *sum-product*. The former is excellent for interpreting the consequent of an "If - Then" rule but loses accuracy in this application. Therefore, the sum-product approach has been used, which, although computationally slower than the other method, does retain the level of accuracy required for this application. A "centre-of-gravity" via a binary search procedure has been employed for this purpose. Put simply, the region under all of the modified triangles in Figure 7.5 is calculated to yield the total area. A starting point of $\frac{1}{2}(C_{VL} + W_{VL})$ or 500, i.e

the centre of the performance index axis (from 0 (low) to $C_{VL} + W_{VL}$ (high) or 1000) is used and the area to the left of this point is calculated. If half of the total area is greater than this, the centre is moved to the mid to high region, i.e. from 0 to 1000 to 500 to 1000. The converse happens if the calculated area is greater than half of the total area. This process continues until the two regions are equal to an accuracy of 0.01, where the midpoint that has been calculated is equivalent to the pivot or fulcrum of the total area and it is this that is the total system performance index for that contingent quantity. In Figure 7.5, it can be seen that the total system performance index at this point will be more biased towards the left hand side of the plot, since it is dominated by the *Small* linguistic variable.

An average value of the total system performance index for each contingent quantity after every contingency analysis period is summed together with the other quantities to give the total system severity index, so that

$$SI_{Total} = PI_{Line} + PI_{Busbar} + PI_{Group} + PI_{MVAr} \tag{7.3}$$

where PI_{Line}, PI_{Busbar}, PI_{Group} and PI_{MVAr} are the final total system performance indices for line flow, busbar voltage magnitude, group output power and MVAr injections into the network respectively. This number is then passed back to the *Application Routine* to be stored with its associated system and stability alarms for ordering and printing.

7.3.1 Ranking and Results Processing

Once all of the contingencies have been applied from the database, the processing of the stored results begins. The first two contingencies stored are accessed, releas-

ing that portion of memory that these contingencies occupied. Ordering between these results is achieved by comparing the total system severity index for each. A reverse ordering procedure has been used, so that if the first result has a total system SI less than the second, it is placed above the latter in a pseudo ranked list in memory. This process continues until all of the contingencies that have been stored have been "downloaded", so that the most severe is placed at the bottom of the ranked list in a stack type structure in memory.

When the results are ready to be presented, the bottom of this stack is accessed first and printed either to screen or to file on the hard disk of the computing system being used. Since for larger systems, many contingencies may be present in the final output, the latter form of results presentation has been preferred, although development of an X Windows interface may prove a satisfactory solution.

Each contingency is printed together with its associated network violations and stability alarms in one of three formats, namely a full alarm list, a reduced set of warnings grouped in geographical areas where the violations occur and a general summation of the alarms that appeared during the contingency. This alarm processing will be described in more detail in a following section. At the top of each results file is a measure of the number of line, busbar, load and group contingencies together with an indication of the solution time for the complete security assessment cycle of the whole database. These formats will be discussed in more detail in the next chapter.

7.4 Stability Assessment

An evaluation of power system stability is an essential function of a security assessment tool during contingency analysis. Because of this, a transient and dynamic

instability identification algorithm has been developed based on the concept of fuzzy-set techniques used in the previous section. Each mode of instability has been treated as a separate issue, i.e. during both the contingency screening and analysis periods, transient stability assessment is carried out and, if after this time, power oscillations are still above a threshold value, the contingency simulation is extended to ascertain whether these oscillations damp out, remain at the same level or grow in amplitude.

7.4.1 Transient Stability

During each contingency application, the function used for transient stability assessment is called from the the main calculation loop of the simulator by the contingency *Application Routine.* Three objects are passed to this function and include the machine rotor angle δ, machine rotor acceleration A_{cc} and machine kinetic energy K_{in}.

Each group in the model network is checked every simulation time step and, as for contingency analysis, each of these parameters are calculated and classified in one of four fuzzy sets or linguistic variables. These are principally : -

- Stable
- Critically_Stable_Low
- Critically_Stable_High
- Unstable

Each of these categories is represented by operator-specified "limits". For example,

in the case of machine rotor angle, δ is classified according to its angle swing from its initial pre-contingent position, so that

- Stable - angle swing of 20 to 40 degrees.
- Critically_Stable_Low - angle swing of 40 to 70 degrees.
- Critically_Stable_High - angle swing of 70 to 100 degrees.
- Unstable - angle swing greater than 100 degrees.

This, in itself, can be used as a measurement of transient stability but, there are some cases, in particular pump-storage machines, where the rotor angle swing exceeds 100 degrees and still returns to its original position without pole-slipping. Because of this, two additional measurements are made on rotor acceleration and machine kinetic energy which are classified in a similar way to that for rotor angles.

Once these classifications have been made, a set of "hard-wired" fuzzy reasoning rules are used to make a decision on the group stability. These rules are of the form "If A And B Or C Then D". If transient instability occurs, a warning message is sent to the contingency structure and printed with the rest of the results when all the contingencies in the database have been applied.

This method has proved to be accurate and efficient in terms of computational demand, since the calculation of the contingent quantities is carried out by the simulator main loop every time step and, hence, only rule processing needs to be conducted. In the test described in the next chapter, those cases that were transiently unstable were run off-line and proved 100% accurate. Unlike the direct methods described in section 3.2.2, no approximation has been made of the power

system model, since a time domain solution has been used and, although a direct measurement of the degree of stability is not immediately available, enhancements could be made by introducing more machine parameters and modifying the rule-base to accommodate these changes.

7.4.2 Dynamic Stability

Two modes of dynamic or steady state instability are possible in an electrical power system. As described in Section 3.2.3 of this thesis, these are : -

- *Oscillatory instability*, where power transferred between two regions connected by long transmission lines can start to oscillate and can increase to dangerous levels for generator plant and other equipment.
- *Aperiodic instability*, where system variables increase or ramp against one another.

Both of these modes can be detected using the simulator PowSim during contingency analysis. As mentioned previously, if after this analysis period power oscillations or parameter ramping are detected, a further user-specified time interval is used to assess whether the system will ultimately go unstable.

For oscillatory instability, a single parameter is used, that of machine rotor angle, although generated power could be utilised just as effectively. A threshold value is set, below which the system is deemed to be stable. If after the full contingency analysis period, rotor oscillations are still present and above this threshold level, further simulation is carried out. If these oscillations die out during this additional time period, the simulation is halted, or if they remain sustained or start to

increase, the simulation continues until the interval has elapsed and a message is printed to the contingency structure indicating the instability.

A similar approach to that for transient instability detection is carried out, so that the amplitude of the rotor angle oscillation with respect to the threshold level[2] is categorised in one of three classifications, i.e. Damped (D), Sustained (S) or Increasing (I). The amplitude stored in the previous call to this function (made every 5 simulation time steps) and its classification are compared with that of the present conditions. Again rules of the type "**If A And B Then C**" are used to yield a decision on the system stability. During testing of this algorithm, it was interesting to notice that the frequency of these oscillations is very low, typically 0.2 to 1.3 Hz, which has been confirmed by National Grid Company in some of their off-line studies. This extra parameter could be used at a later stage as an additional variable in the rule-base.

For aperiodic instability, all the "integrable" machine states calculated in the main simulator loop are stored every time this function is called. These include direct and quadrature axis voltages (behind sub-transient reactance), field and AVR excitation stabilising voltages, mechanical and electrical torques and governor steam control valve position. A comparison is made between the stored values from the previous iteration and those of the present operating conditions. If a set of parameters are continuing to ramp against one another over the additional time period allocated for dynamic stability studies, a message is flagged to the contingency structure and subsequently printed out with the rest of the results.

---

[2]The threshold value used is 2 degrees rotor angle swing from its last peak to its present trough

7.5 Alarm Handling

In order to aid the operator in the task of producing a set of corrective actions for problem contingencies that are flagged by the security assessor, an alarm processor should be present to indicate the affected areas of the power network. A method loosely based on fuzzy set notations has been developed (as in Figure 3.2) to handle and process system violations. It can be split into two groups, namely data acquisition and information processing.

7.5.1 Data Acquisition

As described in Section 3.3.2 of this thesis, messages coming from the power system need to be categorised into groups of increasing severity as shown in Figure 3.1.

A number of quantities are measured around the network model every simulation time step during the application of a contingency and include : -

1. Busbar voltage magnitudes.
2. Power system frequency.
3. Generator group real power (MW) limits.
4. Generator group reactive power (MVAr) limits.
5. Transmission line MVA power flows.
6. Network topology.
7. Transmission line and group transformer taps.

The procedure for all of these variables is very similar in that directly measurable quantities are normalised, as in Section 7.3, and classified in one of the security levels illustrated by Figure 3.1, i.e.

1. Busbar voltage magnitude deviations are categorised by the difference between the voltage magnitude at the busbar and the nominal magnitude of 1.0 p.u.
2. System frequency is the network frequency. National Grid Company directives specify that the frequency should not change by 2% during steady state operation and by 5% under fault conditions. The latter is used for contingency analysis.
3. Group power generation is classified according to the group's MW and MVAr rated limits.
4. Line power flows in MVA are categorised by the percentage overload with respect to their associated thermal MVA limits.
5. Transformers are present on all lines and generator sets and their tap deviation from the nominal tap position of 1.0 p.u. is monitored.

For network topology checking, a more detailed analysis is required. The procedure is that a busbar is picked as a starting point and all the transmission lines and/or supergrid transformers attached to this node are tested for their connectivity. The process continues recursively for all busbars in the network connected to this first one, until all have been checked. If the system is fully connected, a flag "Islanded" is set to `FALSE`, otherwise, if a node is found to be detached from the network, the flag is set to `TRUE` and the security level is assigned to *LEVEL 5*

For those cases that fall into security *LEVEL 5*, i.e. a non-correctable emergency

where all load is supplied but the system cannot be restored without loss of some of this load, a message is sent directly to the main alarm processor routine and stored for subsequent evaluation once the contingency application has elapsed. Other security levels are processed locally by the relevant data acquisition functions, where "hypotheses" are generated, i.e. to ascertain whether the severity of a particular alarm will increase with respect to its surroundings and present operating conditions.

7.5.2 Information Processing

At the end of each contingency analysis period, the unresolved alarms, i.e. those that have not reached security *LEVEL 5* are processed and queued in memory in the structure associated with that contingency.

Once all the contingencies have been applied from the database, this queued list of alarms is printed together with any stability violations associated with that contingency in the ranked order of final results.

As previously mentioned in Section 7.3.1, the alarms that are printed can be in one of three forms. A full list of violations, together with the percentage deviation from the plant's respective limits is available. This is a very thorough examination of the system state during each contingency and is perhaps too detailed for on-line use. Hence, two alternatives have been developed which progressively summarise the information content. One of the modifications made to PowSim was the introduction of geographical area recognition of the network, e.g. Scotland, North Wales, South West, etc ... From NGC's "National Control" prospective, these areas have been enhanced to include the "Area Control Centre" regions, e.g. London, Bristol, Birmingham and Leeds. Thus a number of voltage alarms that

occur during a contingency in a particular area can be summarised by "`X voltage violations in the London area`". The other result presentation ignores the geographical regions and simplifies the alarm messages to "`Y line overloads`". This is perhaps too concise for on-line control room use but, more effort will have to be made to determine the extent of information that would be needed by an operator in formulating a set of corrective actions.

7.6 Chapter Summary

This chapter has described the software implementation of a dynamic security assessment algorithm. The development has been split into three main parts, namely security analysis, stability assessment and alarm processing.

The security analysis software has been described in some detail illustrating the influence of fuzzy-set techniques in contingency screening and subsequent analysis based on a number of contingent quantities such as busbar voltage magnitudes, line flows, generator power outputs and MVAr injections into the network from these generating groups and are classified into five linguistic variables. With the aid of fuzzy set notation, the membership functions of these sets can be manipulated in such a way as to yield the total system severity index for each contingency.

Stability assessment has been developed for both transient and dynamic/steady state analysis. Again, an adaption of the fuzzy-set techniques has been used to make decisions about the system's stability based on rotor angle, rotor acceleration and machine kinetic energy for the former and rotor angle amplitude of oscillation and interaction between machine parameters for the latter.

An essential part of a security assessment program is an alarm processor which

handles vast quantities of system violations during contingency analysis. Three versions of alarm output have been developed which are printed to files together with the associated ranked contingency on the hard disk of the computing system being used.

The next chapter will describe the network modelled and the results that have been collated using this security assessment algorithm.

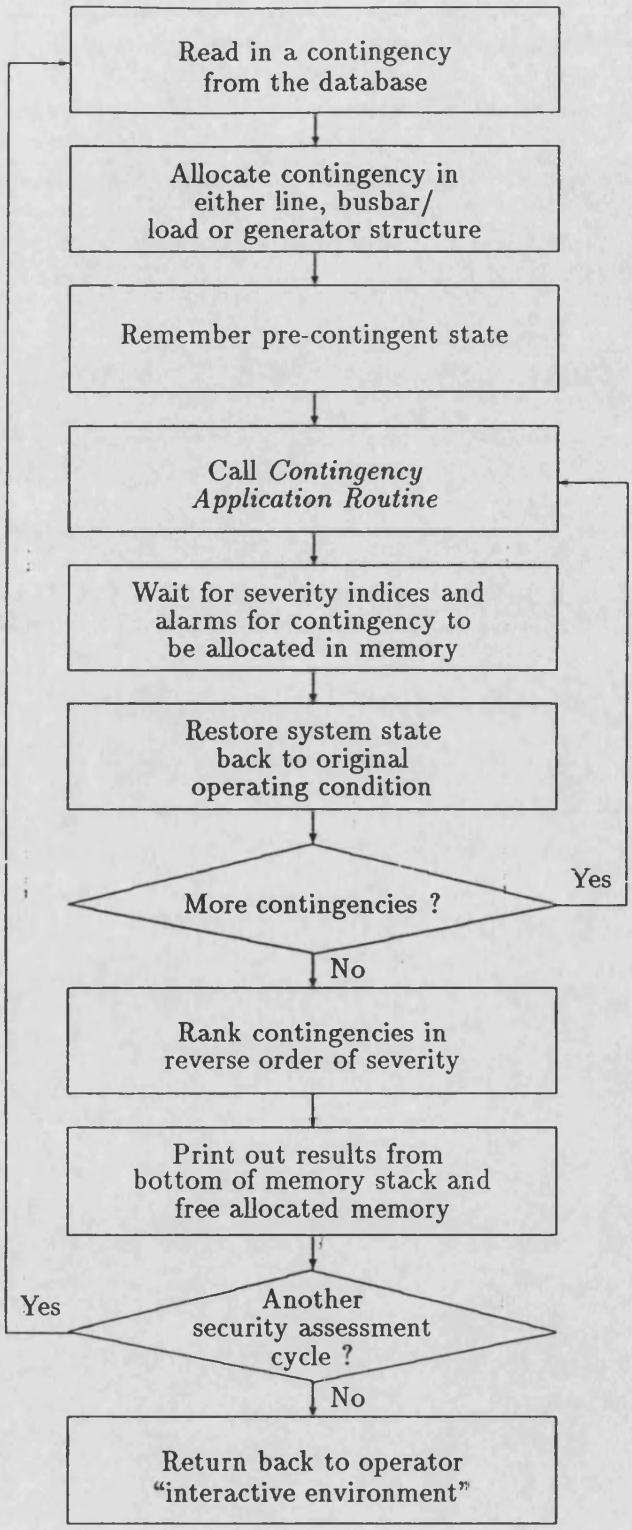


Figure 7.1: Main Contingency Application and Analysis Loop

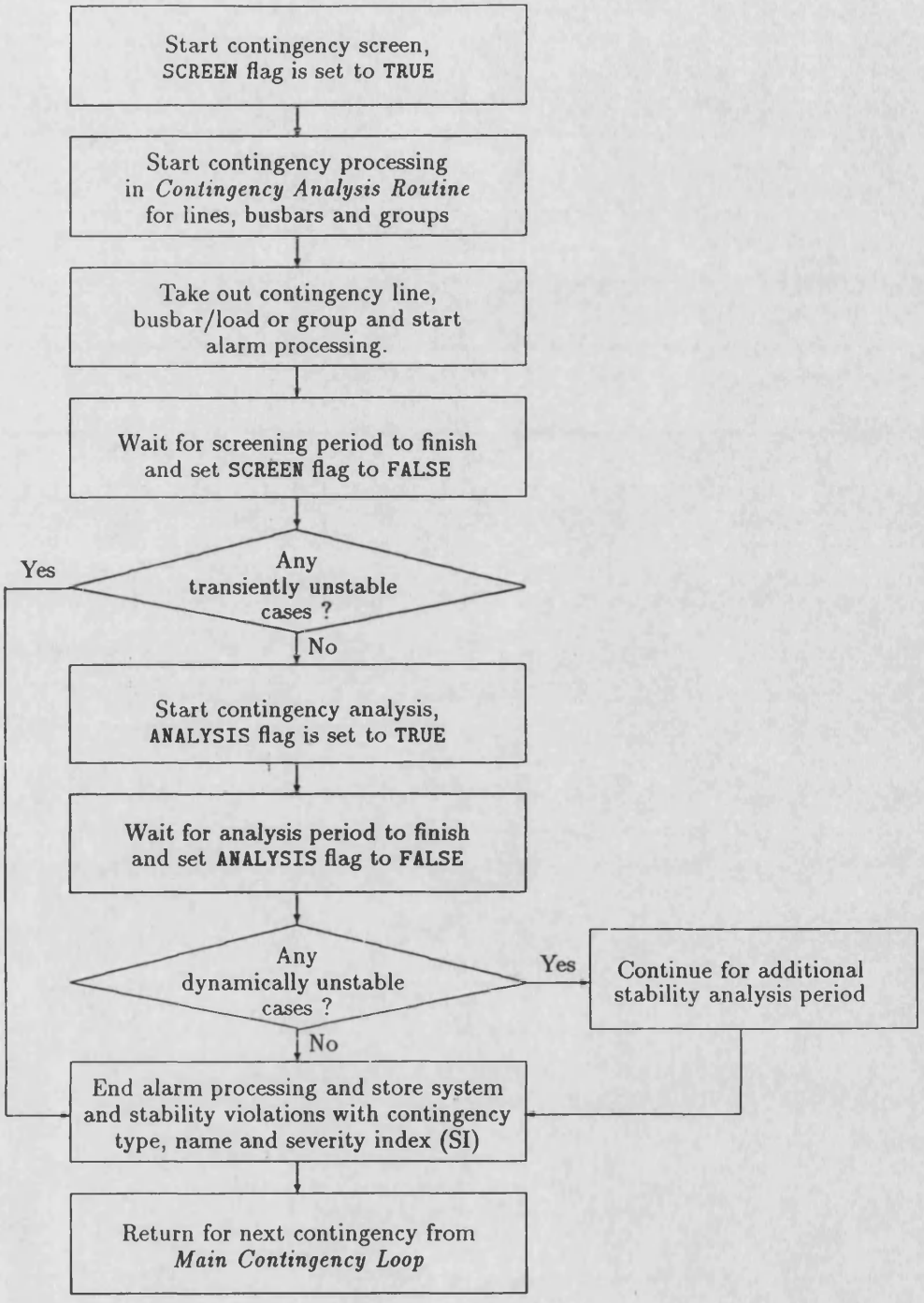


Figure 7.2: Contingency Application Routine

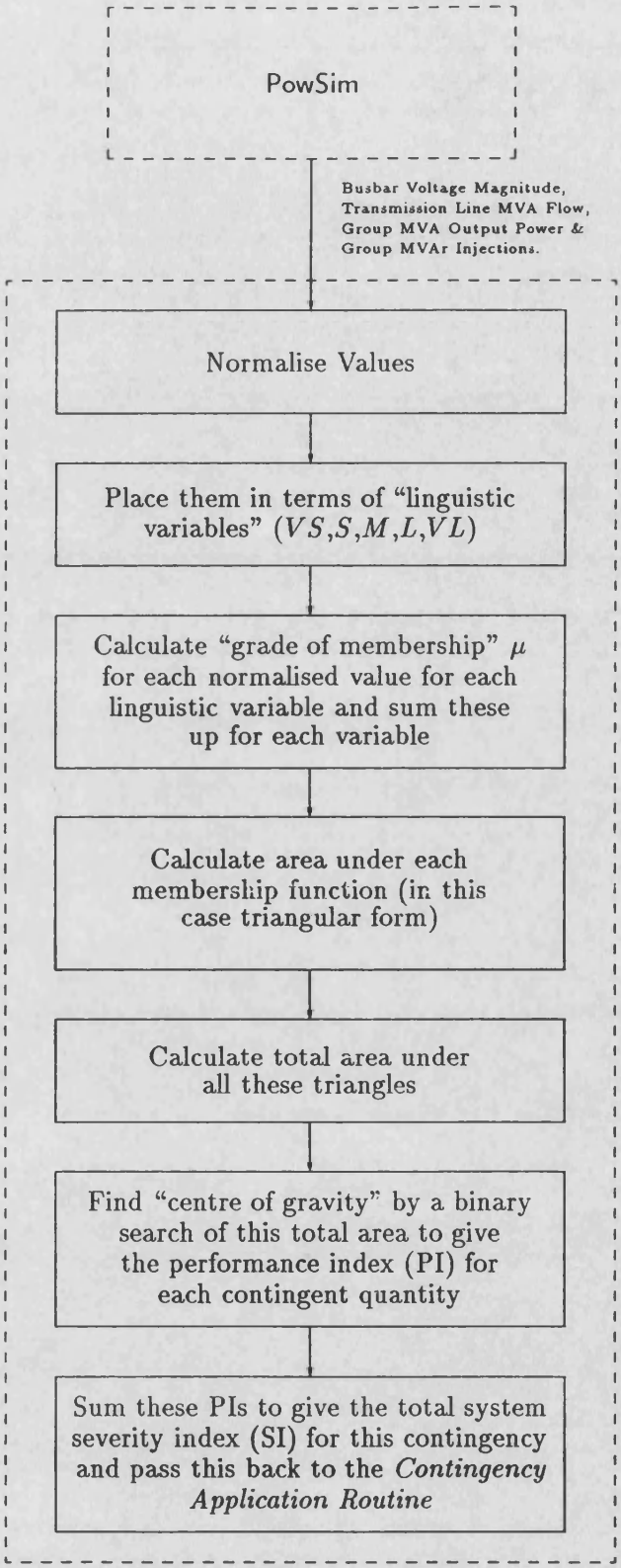


Figure 7.3: Fuzzy-Set Based Contingency Analysis Algorithm

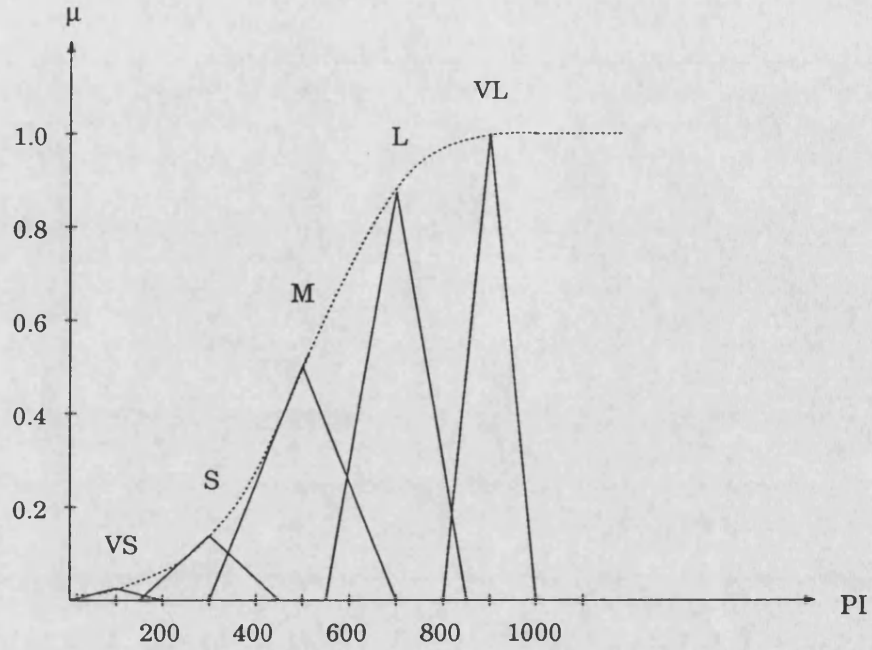


Figure 7.4: Membership Function (μ) vs Performance Index (PI) using a Sigmoid Weighting Function

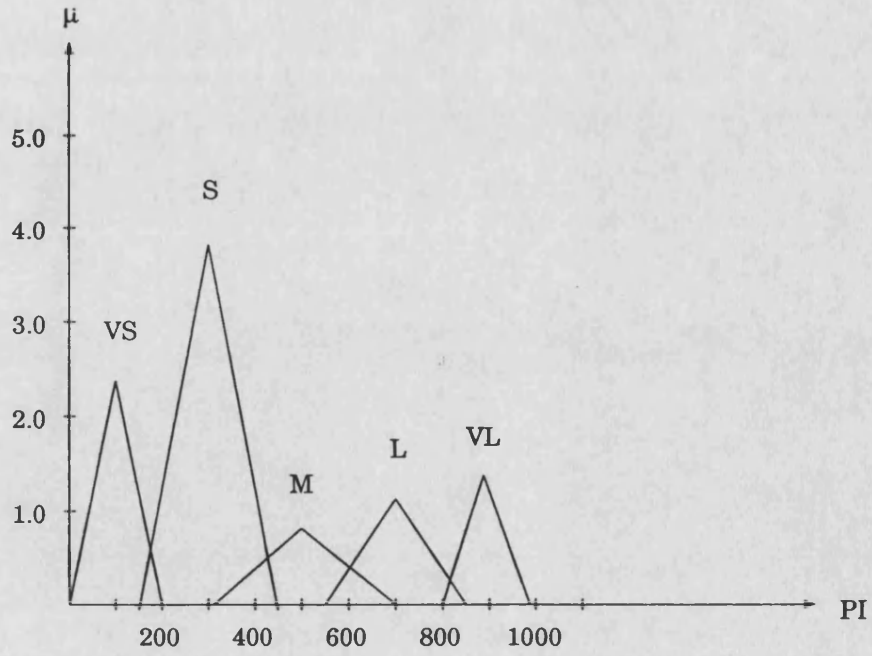


Figure 7.5: Membership Function (μ) vs Performance Index (PI) post-contingency

Membership Function Description		Weighting Approach for Membership Function			
Linguistic Variable	Parameters	Constant $\mu = 1$	Linear $\mu \equiv PI$	Exponential $\mu = e^{5 \cdot PI}$	Sigmoid $\mu = \frac{1}{1+e^{-PI}}$
	C (centre)	100.0	100.0	100.0	100.0
Very Small	W (width)	100.0	100.0	100.0	100.0
	P (peak)	1.0	0.20	0.018	0.02
	C (centre)	300.0	300.0	300.0	300.0
Small	W (width)	150.0	150.0	150.0	150.0
	P (peak)	1.0	0.40	0.049	0.12
	C (centre)	500.0	500.0	500.0	500.0
Medium	W (width)	200.0	200.0	200.0	200.0
	P (peak)	1.0	0.60	0.134	0.50
	C (centre)	700.0	700.0	700.0	700.0
Large	W (width)	150.0	150.0	150.0	150.0
	P (peak)	1.0	0.80	0.360	0.88
	C (centre)	900.0	900.0	900.0	900.0
Very Large	W (width)	100.0	100.0	100.0	100.0
	P (peak)	1.0	1.0	1.0	1.0

Table 7.1: Membership Function Descriptions and Weighting Methods

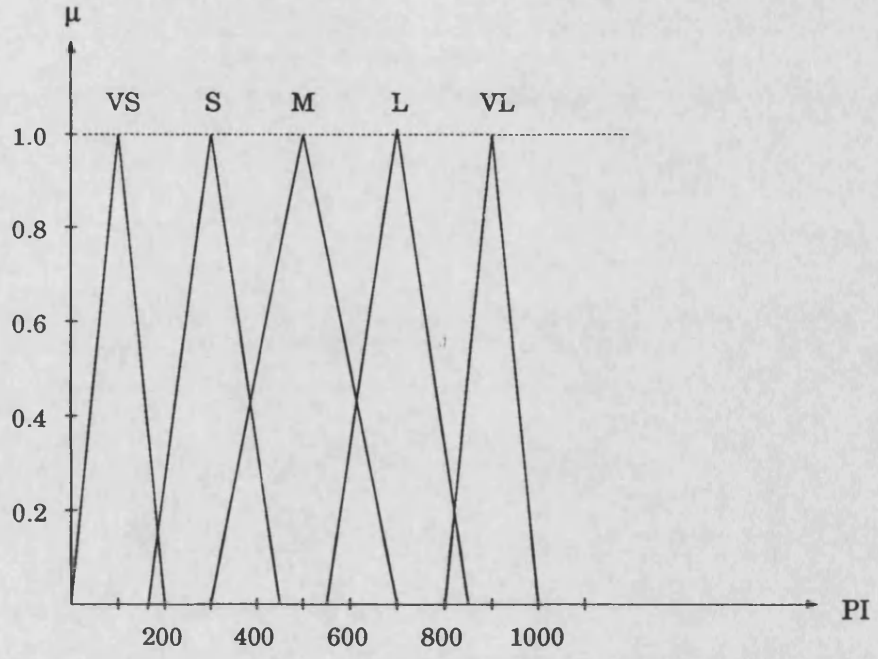


Figure 7.6: Membership Function (μ) vs Performance Index (PI) using a Constant Weighting Function

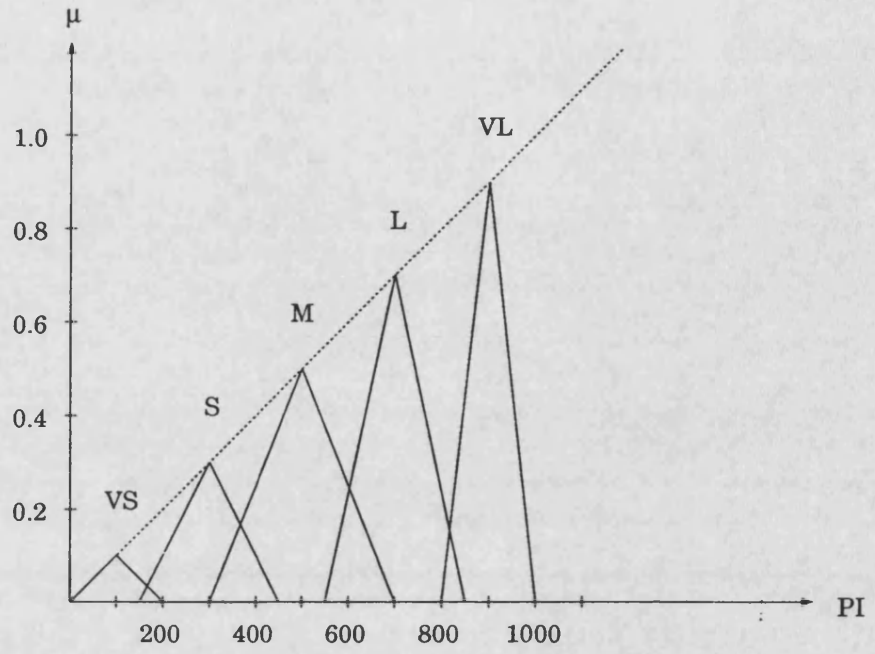


Figure 7.7: Membership Function (μ) vs Performance Index (PI) using a Linear Weighting Function

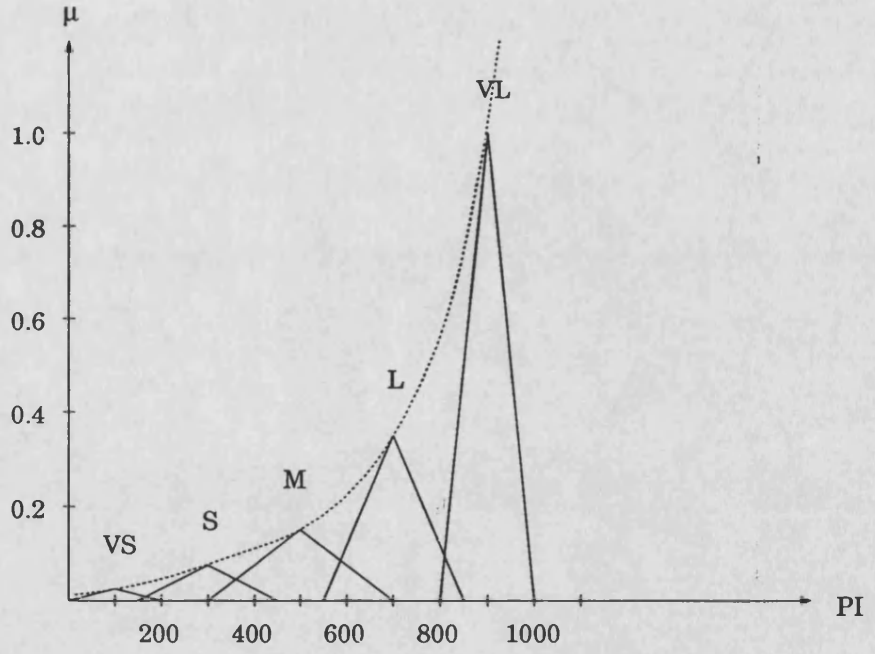


Figure 7.8: Membership Function (μ) vs Performance Index (PI) using an Exponential Weighting Function

Chapter 8

Discussion of Results

8.1 Introduction

A number of test network models that could be run by the power system simulator PowSim were used to examine the performance of the fuzzy security assessor. These systems are : -

- A 4 machine and 6 busbar reduced model of the National Grid system.
- A 20 machine and 100 busbar reduced model of the National Grid system.
- An IEEE 57 busbar test network.
- A full "reduced" National Grid system as used in loadflow and stability studies at the NGC.

Contingency databases for each of these networks were constructed to include all single and double transmission circuit outages, a combination of these, all busbar faults, load losses and generator group trips. Results from each of these systems will be described in the following sections. Comparisons are made between the four fuzzy-set approaches, i.e. constant, linear, exponential and sigmoid weighting functions and a numerical method. Two versions of this latter approach have been

used. The exponent "n" from Equation 2.1 has been set to 2 and 20 respectively. The former is to illustrate the masking effects, discussed in Section 2.4, that occur with a low value of n.

It should be noted at this point that there have been very few publications on fuzzy sets applied to contingency ranking. Of these, comparisons between the new methods and more traditional numerical techniques have been rather "thin" and, in some cases, non-existent. Therefore, in this research, the higher order exponent numerical algorithm has been used as the "benchmark" for the fuzzy-set approaches. This, as discussed previously, has been proved to be free from any errors.

Results are quoted with timing measurements for each security assessment approach. This measurement is taken as the time required to read in the contingency database, apply all the contingencies and finally print out the results to a file on the hard disk. These timing measurements are for the version of the simulator PowSim running on the Microway Number Smasher-860 accelerator card based in a 386 PC. The Silicon Graphics Indigo version, produced exactly the same results but, with an inherent speed up of execution of approximately 2.5 times.

8.2 4 Machine and 6 Busbar Studies

The 4 machine and 6 busbar model was used principally as a test bed for the research. It is a reduction of the UK National Grid system used by Dale [168] and displays all the dynamic characteristics of an fully interconnected electrical power system. Figure 8.1 shows the schematic diagram of this network. Three "conventional" thermal generating groups are connected, equipped with governors and fast automatic voltage regulators. A "pump-storage" machine, that named as

DINORWIG, is also included, since this shows considerably different characteristics to the thermal plant named as CEGB, SCOTLAND and NWALES respectively.

A contingency database was built up to include all the elements mentioned in the Section 8.1. Initially, prior to discussion with staff of National Grid Company (NGC), there were only 19 line contingencies present in the database. With the introduction of the approach used by the NGC in their transient stability studies, as described in Section 7.2.2, the number of line contingencies effectively doubled. This is because both local end and remote end primary tripping cases need to be considered. The final database shows a total of 38 line, 6 busbar, 6 load and 4 generating group contingencies.

Tables 8.1 and 8.2 show a comparison of the results obtained from this network and contingency database for two scenarios. The first is a "summer night-time" loading condition or base case and the second is an operating state where more power is being transferred from the SCOTLAND generator to meet an increase in demand from the rest of the system (essentially England and Wales).

8.2.1 Base Case Condition

All the contingencies in the database for this study were applied using the code developed and described in the previous chapter. Results were produced in one of the three formats mentioned earlier, depending on the alarm processing specifications. These were written to files on hard disk for each of the security assessment algorithms, with the results summarised in Table 8.1.

As mentioned previously, the numerical approach ("$n = 20$") is used as the benchmark for the other methods, which is why there are no entries in the misranking

columns. A number of comparisons can be made from Table 8.1.

It can be seen the solution times for each of the fuzzy-set approaches are approximately the same and are effectively 41% quicker than that of the benchmark. The "$n = 2$" numerical method is also faster (32%) which is due to the decrease in computation.

There were no dynamic/steady state instability violations caused by the application of these contingencies, in this base case condition. However, 15 contingencies did cause transient instability. Using the geographical area specific alarm processing output as an example, a transiently unstable contingency appears in the final output as : -

Contingency	Limit Violations/Alarms	System Stability
Line DEES4-CEGB4:L1 (Remote End Tripped)	1 Group pole-slipped (North Wales) 5 Line Overload Violations (North Wales) 1 Line Overload Violation (England) 4 Voltage Violations (North Wales) 1 Voltage Violation (England) 2 Voltage Violation (Scotland) 1 System Frequency Violation 1 Group MW Limit Violation (North Wales)	Transient Instability

The generating group that pole-slipped in this case was DINORWIG as in Figure 8.2. In some cases NWALES also lost synchronism with the rest of the system.

Compared to the benchmark, there are a number of misrankings in the "$n = 2$" approach. In the first ten ranked contingencies, three were misplaced, two of which were not even in this interval. This consequently affected the ranking of the first twenty contingencies in the final list and can be explained by the masking effect.

The fuzzy-set algorithm based on the constant weighting function, as in Figure 7.6, was equally as bad as this lower order numerical approach. The accuracy, as com-

pared with the benchmark, increased with the introduction of the linear weighting factor. The best results were obtained from the sigmoid function, although the exponential approach used by Hsu et al. [41] was also reasonably valid.

It should be noted that the misrankings involved in these latter two algorithms were purely cases where the ranked contingencies were graded in the wrong order by one place, i.e. a contingency that was ordered no. 6 in the list by the benchmark, was ranked no. 7 by the fuzzy-set sigmoid approach and vice versa.

8.2.2 New Stressed Condition

This additional operating condition was set up by gradually increasing the load on the CEGB4, NWAL4, PENT4 and DEES4 busbars. The generation from the group SCOTLAND was subsequently increased until an equilibrium was reached, i.e. the system frequency was between the NGC steady state limits of 50.2 and 49.8 Hz and there were no self-induced power oscillations between the largest machines in the network.

Table 8.2 summarises the results obtained for each security assessment algorithm, corresponding to this condition.

With the increase in demand and generation, it can be seen from the table that, in addition to the 15 transient instability cases of the base case condition, there were an extra 7 contingencies that caused pole-slipping. This study was set up primarily to test the dynamic stability detection algorithm. The table shows that there were 10 cases of sustained oscillations caused by the contingencies at the end of the evaluation period. Some of these actually caused the system to go unstable, if the time domain simulation was left sufficiently long enough. Figures

8.3 and 8.4 show two examples of oscillatory instability. The top plot is for the "Group NWALES" contingency which causes undamped and sustained oscillations for group SCOTLAND. The lower plot shows hows the oscillations build up from NWALES which ultimately sent the system unstable for the line contingency "Line CEGB4-NWAL4:L1". Again, if the summarising alarm processing output is used, the presentation looks similar to the transient instability cases, i.e.

Contingency	Limit Violations/Alarms	System Stability
Busbar CEGB4	2 Groups with undamped oscillations (North Wales)	Dynamic Instability
	6 Line Overload Violations (North Wales)	
	1 Line Overload Violation (England)	
	4 Voltage Violations (North Wales)	
	1 Voltage Violation (England)	
	2 Voltage Violation (Scotland)	
	1 System Frequency Violation	
	2 Group MW Limit Violations (North Wales)	
	2 Group MVAr Limit Violations (North Wales)	

The speed up produced by the fuzzy-set approaches shows a 38% increase compared to the benchmark. The "$n = 2$" numerical method was also quicker by 31%, for the same reasons mentioned in the base case study.

As before, the lower order numerical algorithm also fell down on the contingency rankings for this condition. A total of 13 misrankings was observed, compared with that of the benchmark, 7 of which were in the first ten places. Again the accuracy of the fuzzy-set approaches increases moving down Table 8.2. The sigmoid weighting function method, in particular, displays only three rankings that were out by one place in the list.

Dynamic instability cases were ranked by the "sigmoid fuzzy-set" method and "$n = 20$" algorithms in Table 8.2 directly below the transiently unstable contingencies. Most of the misrankings from the other fuzzy-set approaches and the "$n = 2$" method were, in part, due to the fact that conditions where sustained or increasing

oscillations were present, were not always highlighted with as much importance. This is mainly because of the lack of a suitable weighting function for the first fuzzy set approaches, in Table 8.2, and the masking effect for the lower order numerical method.

8.3 20 Machine and 100 Busbar Studies

The 100 busbar network shown in Figure 8.5 is an enlargement of the 60 busbar model used by Berry [169] which was reduced from a much larger scale system study. This full system consisted of 686 nodes, 30 of which were connected with active generation and 5 pumped-storage sites, and 1642 lines, of which 644 were shunt reactors. A static reduction program RACE01 [186] was used to reduce this system to 60 nodes, with 20 of these as active generation and/or motoring loads, and 182 lines with 9 shunts. This reduction was later modified to incorporate more interconnecting nodes in the south east of England and the south of Scotland, as in the real UK high voltage transmission system. The same number of machines have been used which include two pump-storage machines in North Wales, Dinorwig and Ffestiniog, as well as hydro-electric generators in Scotland.

The contingency database for this study was, again, built up to include all single, double and triple circuit line outages, busbar faults, load and generation losses. NGC also gave advice on additional combinations of contingencies which could cause transient, dynamic and/or voltage problems in this reduced network. These include major tie-lines between Scotland and England, the main transmission routes from the generation rich north and the load affluent south, as well as inter-area tie-lies in the south. This results in a database that contains 634 line, 100 busbar, 100 load and 20 generator group contingencies.

As for the 4 machine and 6 busbar study, two scenarios were set up for a base case condition (summer night-time loading) with a power transfer from Scotland to England of 500 MW and an increased power transfer of approximately 920 MW from the Scottish network to meet demand in the south east of England.

8.3.1 Base Case Condition

Table 8.3 shows the comparison of results between the different security assessment algorithms corresponding to this operating condition.

Out of the total 854 contingencies, 721 passed through the system alarm and stability violation detection filter and ranked according to their relative severities. It can be seen from Table 8.3 that there is an increase in computational speed for both the numerical "$n = 2$" method (28%) and fuzzy-set approaches (44%). The increases for both of these are approximately the same as those recorded for the 4 machine and 6 busbar study. The "$n = 2$" method has decreased slightly, whilst the fuzzy-set algorithms have actually increased. This is possibly due to the fact that with the extra data coming from the simulator, the processing power needed for numerical calculation would be much greater than the fuzzy-set classification method.

22 contingencies were highlighted by all the algorithms to be transiently unstable, with no dynamic stability problems detected. All the cases that were unstable were run off-line on the simulator to verify the results.

Again misrankings are evident, when comparing the two numerical approaches. As for the smaller study, not all transiently unstable cases are ranked at the top of the list by the lower order algorithm. This is also true for the fuzzy-set approaches

high in Table 8.3. Those methods, i.e. exponential and sigmoid functions, that are heavily weighted to the *Medium/Large* to *Very Large* regions very closely resemble the results produced by the benchmark.

As mentioned previously, the only misrankings that are present between the sigmoid fuzzy-set method and the benchmark are out by one place in the final ranked list of contingencies.

8.3.2 New Stressed Condition

As for the 4 machine and 6 busbar study, an additional scenario was set up to detect any dynamic instabilities that may occur during the analysis of a contingency. Again the load was increased in the southern half of the English network, with the demand met by the Scottish generators. This was facilitated by decreasing the load on the hydro-electric machines, i.e. effectively taking them out of "motoring" mode. A stable condition was finally met where any further increase in power transfer from Scotland to England would set up oscillatory instability in both interconnected areas.

Table 8.4 shows a comparison of the results for each of the security assessment algorithms. As for the smaller reduced model, a number of contingencies that caused dynamic instability were highlighted. Most of these were, in fact, the cases suggested by the NGC, that for a suitable loading condition, could result in dynamic instability. There was also a corresponding increase in the number of transiently unstable contingencies. This is due to this new operating condition which stresses the power network far more than the base case study. Generating groups are naturally nearer to their respective stability limits and, hence, the tendency for them to pole-slip is correspondingly higher. A large percentage

of these transiently unstable cases showed dynamic instability properties. This means that power oscillations that built up, from the start of the contingency, sent the system unstable shortly after the analysis time period had elapsed. It was considered that this was more of a transient problem than a dynamic one and, hence these contingencies were classified as transiently unstable.

Again, as for the previous study, the pump storage machines, Dinorwig and Ffestiniog, were the predominant groups to go transiently unstable. This was also true for the hydro-electric machines in Scotland. The reason for this can be explained by the presence of fast automatic voltage regulators (for those in North Wales) and slower a.v.r.'s (for those in Scotland) which try to effectively control the terminal voltages of machines with approximately half the inertia of conventional thermal generation plant. Even though the pump-storage machines were most prone to transient instability, it was the thermal generation plant that was the most liable to display oscillatory instability during certain contingencies. A comparison between the two operating conditions, i.e. the base case and this more stressed operating condition for a group contingency, where group HINKLEY is tripped, is shown in Figures 8.6 and 8.7 respectively. The lower plot shows power oscillations building up over the 60 second evaluation period, which would eventually send the system transiently unstable.

The solution times for the fuzzy-set approaches were approximately the same, displaying a 40% computational speed increase compared to the benchmark. As mentioned previously, the accuracy of these methods increases with a "heavier" weighting function, with only a few misrankings between the sigmoid approach and the "$n = 20$" numerical algorithm. The "$n = 2$" method was the least accurate, with a number of cases highlighted by the benchmark in the first ten of the final ranked list which did not appear in the corresponding interval for the lower order

algorithm. This happens for the same reasons mentioned before in Section 8.2.2.

Appendix A shows a typical contingency database used for security analysis on the 20 machine and 100 busbar model network. This database contains 8 line (4 single and 4 double circuit outages), 6 busbar, 6 load and 6 generator group contingencies.

Tables A.1 and A.2, in Appendix A, show comparisons between the results obtained for the two scenarios described in this section, i.e. the base case and the new stressed condition. These tables are a summary of the results themselves and a illustration of the differences that were observed in the final ranked list of contingencies for the two scenarios, respectively.

Typical outputs for these two scenarios are shown in Appendices B and C respectively. These show the format for the three alarm processing files for this example contingency database.

8.4 IEEE 57 Busbar Studies

A network was set up based on an IEEE standard test system which is used primarily for load flow studies [187]. This was modified, to effectively remove the slack busbar and to include seven machines, four of which were treated as thermal generation plant, with the rest acting as synchronous compensators. Figure 8.8 shows the schematic layout of this network. The model was also modified to include a number of double transmission circuits as in the AEP 57 busbar test system, so that a more realistic contingency analysis could be carried out. The database was constructed for this study and included 194 line, 57 busbar, 57 load and 7 generator group contingencies.

Table 8.5 shows the results obtained for each security assessment algorithm. As for the two previous study cases, it can be seen that there is a considerable speed up advantage that can be gained from using the fuzzy-set methods (approximately 50%). An equally high speed up was also achieved by the "$n = 2$" numerical method (43%) as compared to the benchmark. However, a corresponding loss in accuracy was suffered, as mentioned earlier. This speed up is greater than either of those of the previous studies, since the operating condition for this network is relatively unstressed compared to the base case conditions of the 4 machine and 6 busbar and 20 machine and 100 busbar models. This has the effect of reducing the computational demand required for machine and network calculations, i.e. less time is needed to reach convergence for each of the equation calculations.

Interestingly, the fuzzy-set approach with a constant weighting factor, i.e. $\mu = 1$ for all linguistic variables, is actually worse that the lower order numerical method. It shows four misrankings out of the first ten contingencies in the ordered list. Once again, the accuracy of the fuzzy-set algorithms increases moving down Table 8.5.

8.5 NGC Network Studies

A copy of the network parameters used by NGC in their loadflow (OPFL02) and stability (RASM06) studies was modified so that PowSim could run. This full system consists of : -

1. 718 busbars
   (a) 588 load nodes (England and Wales)
   (b) 37 load nodes (Scotland)
   (c) 93 generator nodes

2. 1464 lines

   (a) 1141 transmission lines and transformers

   (b) 323 shunt reactors

3. 93 generating groups

   (a) 88 (England and Wales) including 2 pump-storage schemes

   (b) 5 (Scotland)

The study was based around predicted conditions for the late summer/early autumn period of this year (1994). Figure 8.9 shows the connection diagram of this system. Those lines and boxes (busbars) that are blue correspond to 400KV and those that are black are rated at 275KV. The lines and transformers that have been crossed out in red are items of plant that have been taken out for maintenance and are, hence, pre-contingency outages.

In off-line studies at National Grid House (NGH), Coventry, the load flow program OPFL02 [174] was used to determine the final operating state of this system for a number of double transmission circuit outages. Fifty of these were chosen by experienced staff and the load flow run. From this, for each case, the stability program RASM06 [188] was used to calculate and print the final output plot for a set of user defined variables. In this studies, machine rotor angle (in degrees) and real power generated (in MW) for four machines distributed around the system were used. A "look-up" table is required by RASM06 to determine the switching sequence and protection operation times to remove each of the fifty double circuit outages from the network. This is, in essence, very similar to the switching sequences used for line contingency analysis, as explained in Section 7.2.2. Plots for both local end and remote end primary tripping for each of the double circuit

outages were obtained. These were then visually ranked according to their relative degrees of severity.

This full system, as mentioned earlier, was modified to a format which PowSim could use as its initial start-up file. The contingency database that was built up, consisted purely of these 50 double circuit outages for both local and remote end tripping, giving a total of 100 line contingencies. Table 8.6 shows the comparison of the results for each of the security assessment algorithms. During contingency analysis, as for the off-line studies carried out at NGH, there were no cases highlighted which were transiently unstable. The performance of the benchmark, "n= 20" numerical algorithm, corresponded almost exactly to the "visual" ranking. The trend shown by the previous study cases indicates, again, that the accuracy of the fuzzy-set approaches increase as one moves down Table 8.6.

8.6 Chapter Summary

In this chapter, results have been presented for a number of test systems, displaying the errors that become apparent for different security assessment algorithms.

A numerical approach, with an exponent equal to 20, has been used as the benchmark for the other methods. The main "error producer" was that of the lower order numerical algorithm ("$n = 2$") with a number of misrankings occurring in the top twenty of the final ordered list of contingencies for each study case. This problem was due to the "masking effect" that has been described in Chapter 2.

The fuzzy-set approach with no weighting factor ($\mu = 1$ for all linguistic variables) showed that the number of misrankings that were obtained when compared with the benchmark, made it an impractical method for on-line use. This accuracy,

however, increased with more "severe" weighting factors, with the sigmoid function as the best.

The advantages of using such a fuzzy-set based approach are apparent, since the accuracy of results is comparable to a high order numerical algorithm but with a considerable speed-up in execution times.

The parameters listed in Table 7.1 still need to be fine tuned by an operator or other experienced staff to obtain the exact results required. Although, initial "trial and error" values have been used, the final output, particularly for the full NGC system, was very encouraging.

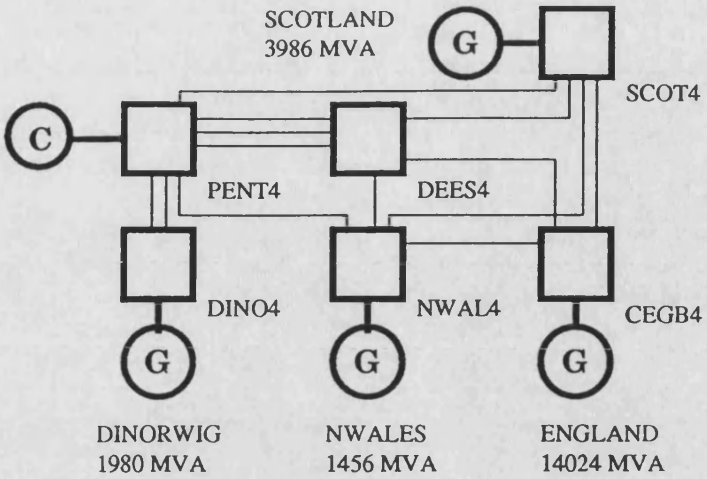


Figure 8.1: 4 machine and 6 busbar reduced study model of the NGC system

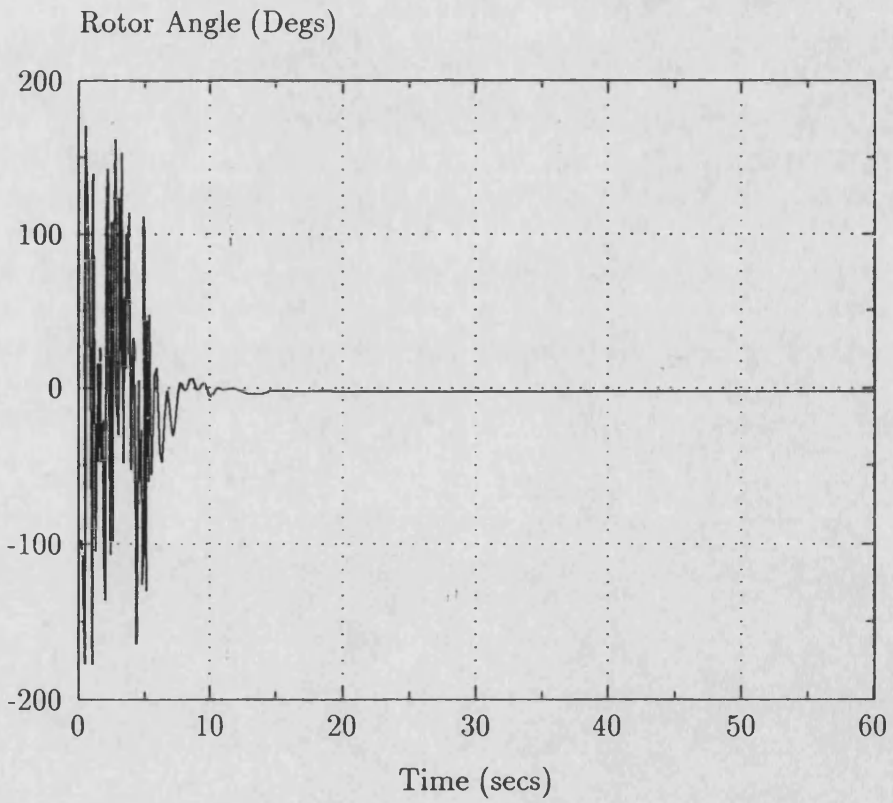


Figure 8.2: Plot of Group DINORWIG Rotor Angle during "DEES4-CEGB4:L1" contingency (Base Case Condition)

Security Assessment Algorithm	No. of Misrankings		No. of Stability Cases		Solution Time in minutes
	1^{st} Ten	1^{st} Twenty	Transient	Dynamic	
Numerical ($n = 2$)	3	9	11	0	0.68
Numerical ($n = 20$)	-	-	11	0	0.82
Fuzzy-Set (Constant)	2	8	11	0	0.62
Fuzzy-Set (Linear)	1	7	11	0	0.61
Fuzzy-Set (Exponential)	1	4	11	0	0.61
Fuzzy-Set (Sigmoid)	0	2	11	0	0.60

Table 8.1: Results for 4 Machine - 6 Busbar Network (Base Case Condition)

Security Assessment Algorithm	No. of Misrankings		No. of Stability Cases		Solution Time in minutes
	1^{st} Ten	1^{st} Twenty	Transient	Dynamic	
Numerical ($n = 2$)	7	13	17	11	2.33
Numerical ($n = 20$)	-	-	17	11	3.47
Fuzzy-Set (Constant)	4	11	17	11	2.13
Fuzzy-Set (Linear)	4	8	17	11	2.13
Fuzzy-Set (Exponential)	3	7	17	11	2.12
Fuzzy-Set (Sigmoid)	1	3	17	11	2.11

Table 8.2: Results for 4 Machine - 6 Busbar Network (Stressed Condition)

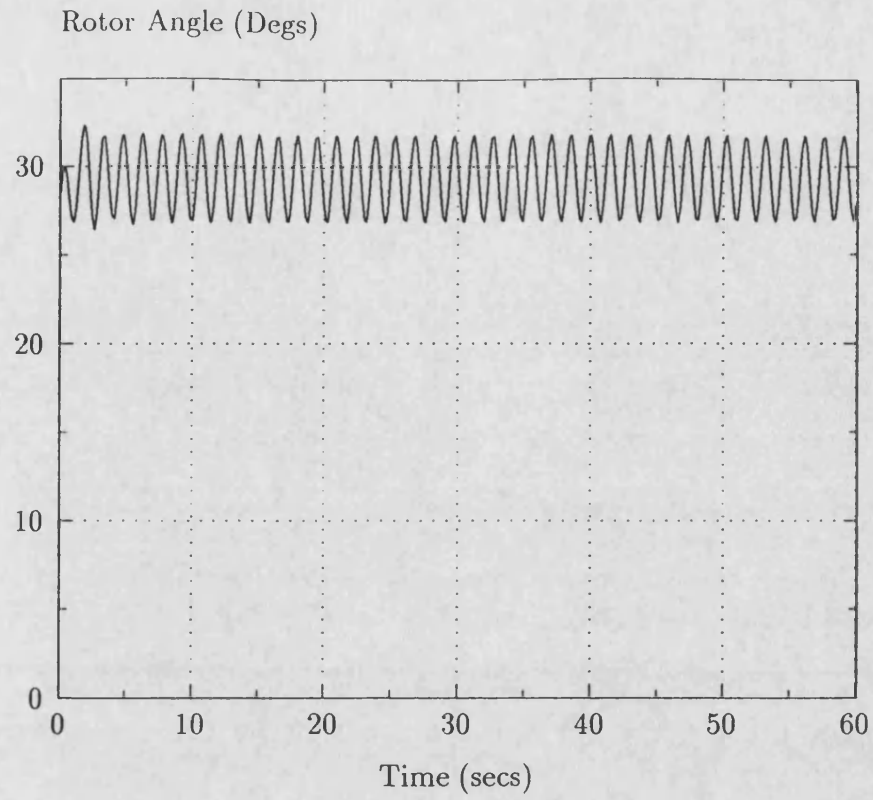


Figure 8.3: Plot of Group SCOTLAND Rotor Angle during "Group NWALES" contingency (Stressed Condition)

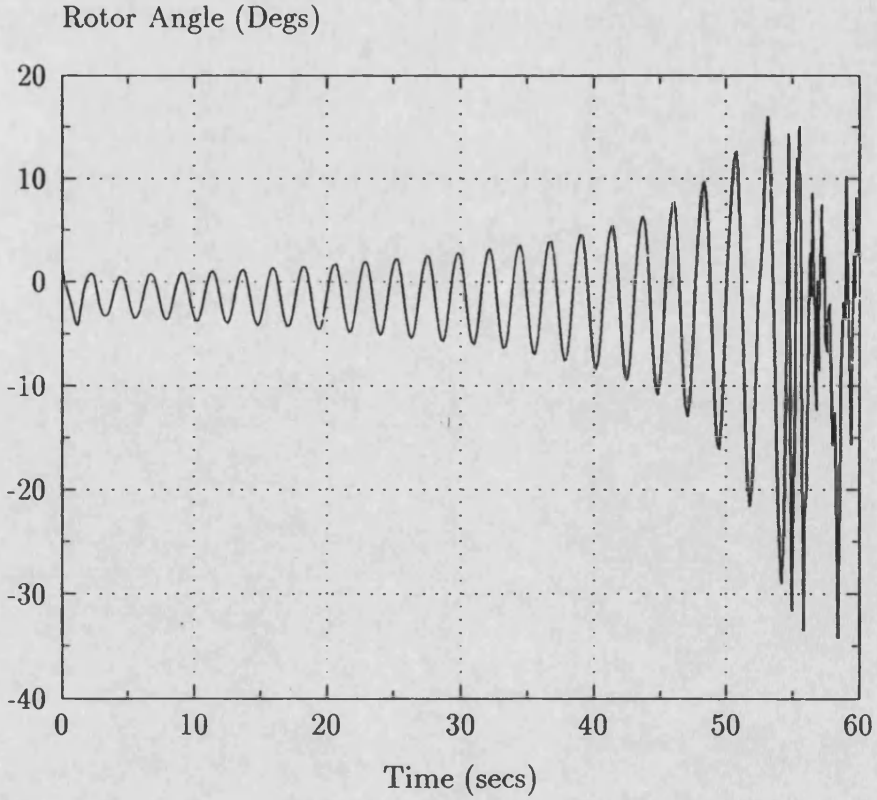


Figure 8.4: Plot of Group NWALES Rotor Angle during "Line CEGB4-NWAL4:L1" contingency (Stressed Condition)

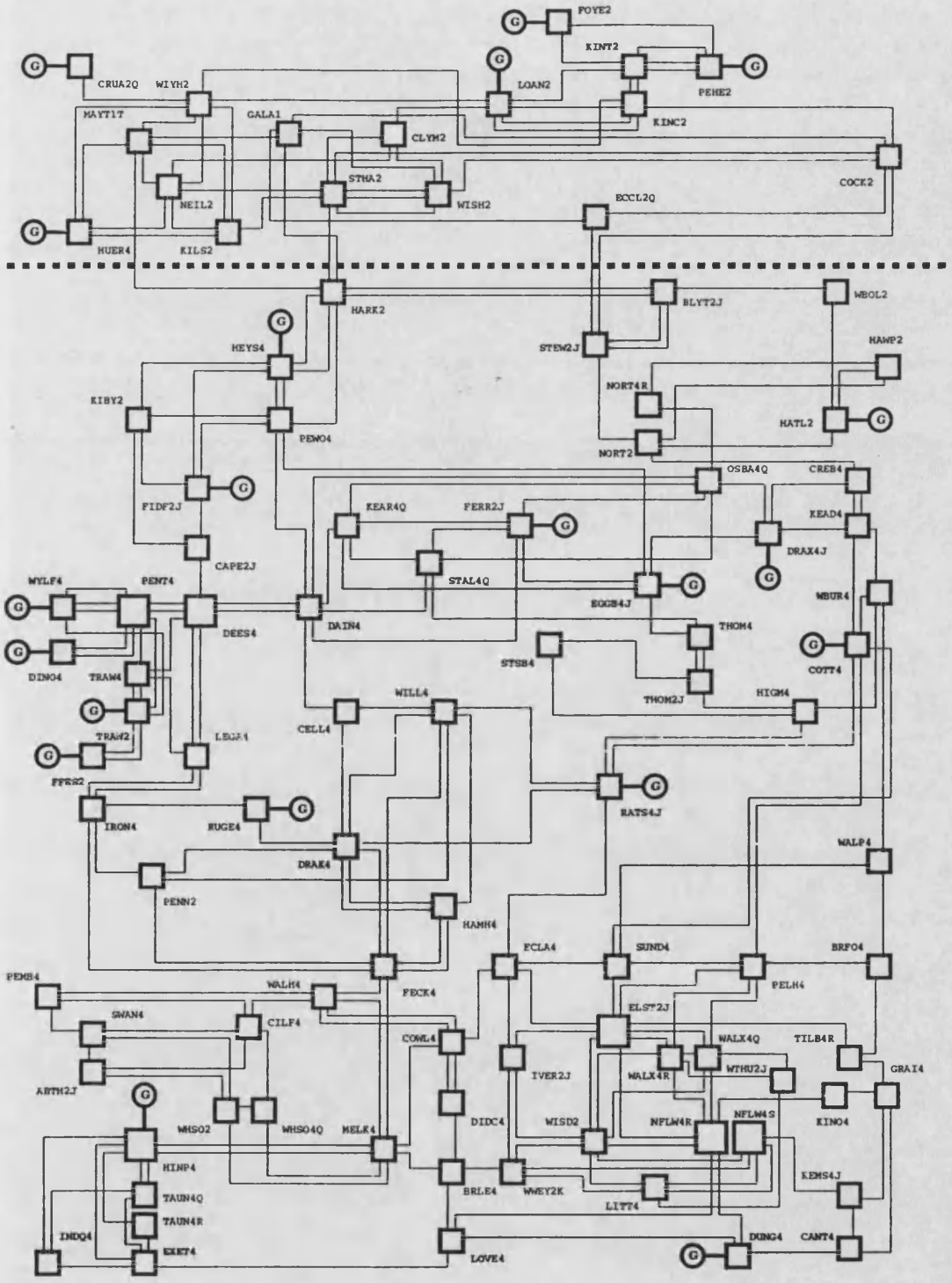


Figure 8.5: 20 machine and 100 busbar reduced study model of the NGC system

Security Assessment Algorithm	No. of Misrankings		No. of Stability Cases		Solution Time in minutes
	1^{st} Ten	1^{st} Twenty	Transient	Dynamic	
Numerical ($n = 2$)	7	13	22	0	92.68
Numerical ($n = 20$)	-	-	22	0	128.26
Fuzzy-Set (Constant)	5	11	22	0	72.16
Fuzzy-Set (Linear)	5	9	22	0	72.15
Fuzzy-Set (Exponential)	2	6	22	0	72.17
Fuzzy-Set (Sigmoid)	2	3	22	0	72.13

Table 8.3: Results for 20 Machine - 100 Busbar Network (Base Case Condition)

Security Assessment Algorithm	No. of Misrankings		No. of Stability Cases		Solution Time in minutes
	1^{st} Ten	1^{st} Twenty	Transient	Dynamic	
Numerical ($n = 2$)	8	15	563	9	193.4
Numerical ($n = 20$)	-	-	563	9	270.48
Fuzzy-Set (Constant)	7	12	563	9	153.37
Fuzzy-Set (Linear)	5	11	563	9	153.35
Fuzzy-Set (Exponential)	4	8	563	9	153.33
Fuzzy-Set (Sigmoid)	3	5	563	9	153.33

Table 8.4: Results for 20 Machine - 100 Busbar Network (Stressed Condition)

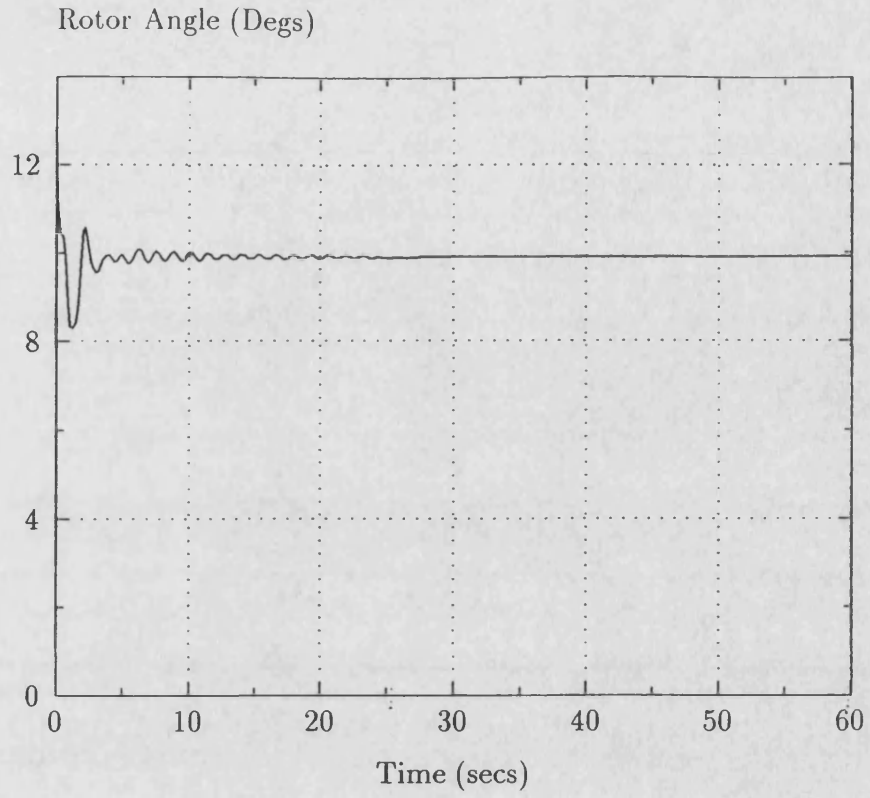


Figure 8.6: Plot of Group COTTAM Rotor Angle during "Group HINKLEY" contingency (Base Case Condition)

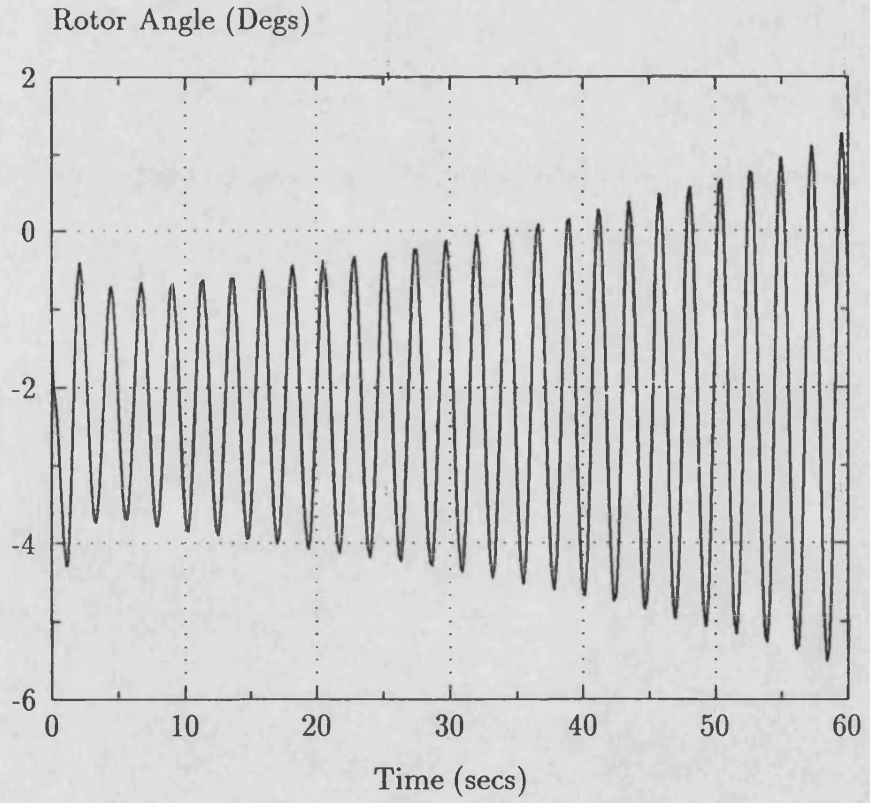


Figure 8.7: Plot of Group COTTAM Rotor Angle during "Group HINKLEY" contingency (Stressed Condition)

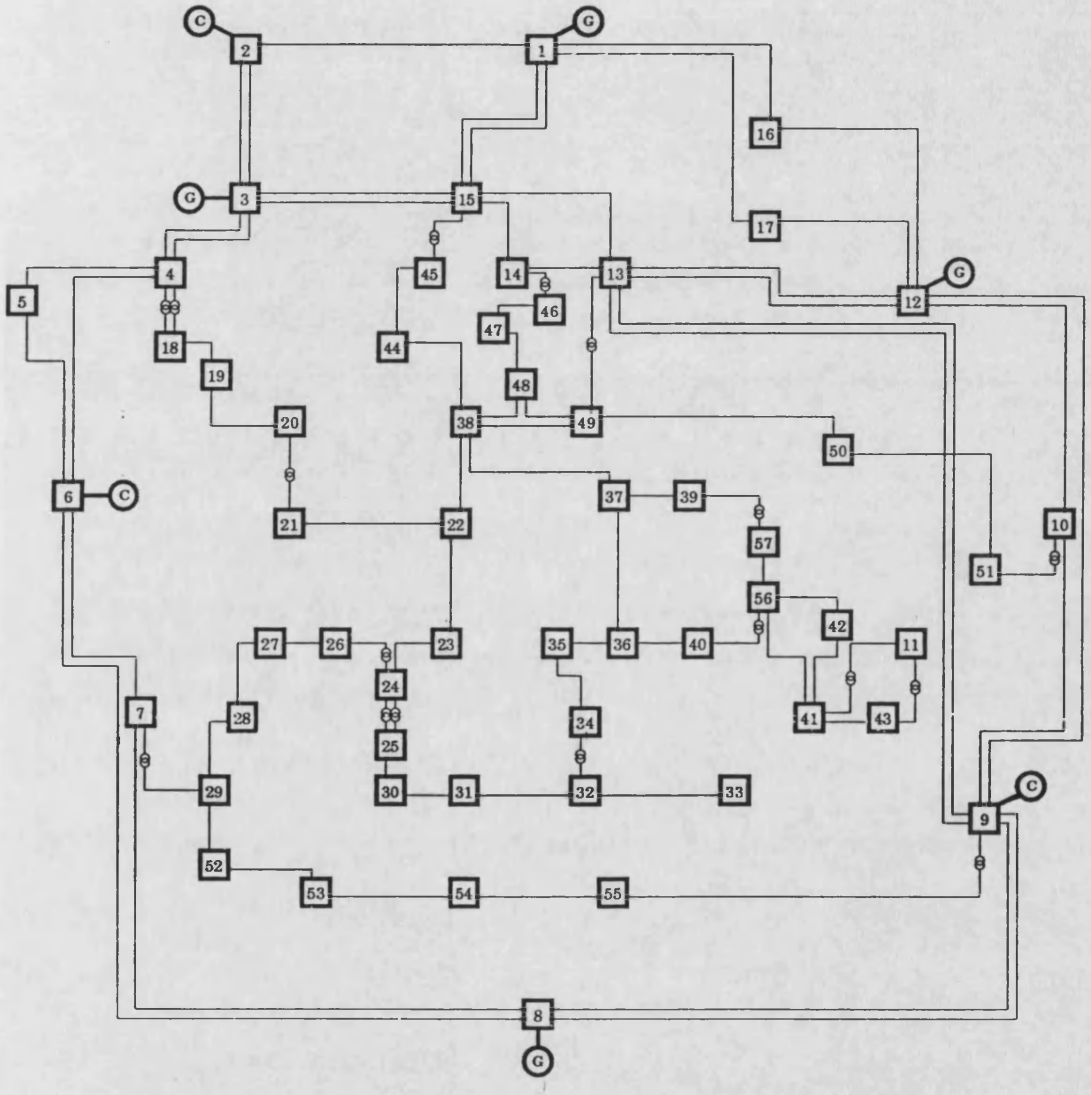


Figure 8.8: IEEE 57 busbar test network

Security Assessment Algorithm	No. of Misrankings		No. of Stability Cases		Solution Time in minutes
	1^{st} Ten	1^{st} Twenty	Transient	Dynamic	
Numerical ($n = 2$)	2	7	0	0	10.93
Numerical ($n = 20$)	-	-	0	0	19.06
Fuzzy-Set (Constant)	4	7	0	0	9.6
Fuzzy-Set (Linear)	2	6	0	0	9.5
Fuzzy-Set (Exponential)	1	4	0	0	9.5
Fuzzy-Set (Sigmoid)	1	3	0	0	9.6

Table 8.5: Results for IEEE 57 Bus Network

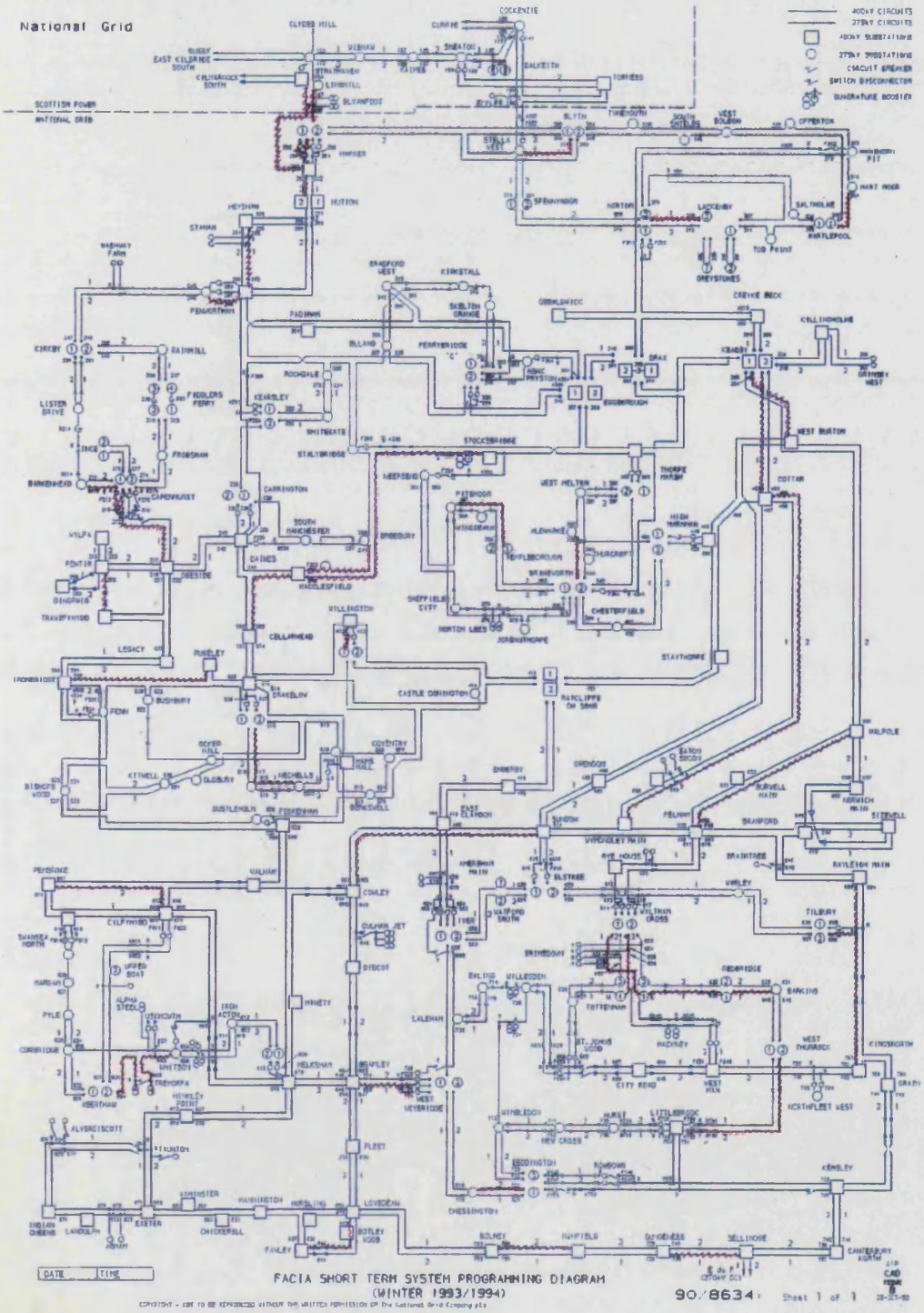


Figure 8.9: NGC system used for OPFL02 and RASM06 studies

Security Assessment Algorithm	No. of Misrankings		No. of Stability Cases		Solution Time in minutes
	1^{st} Ten	1^{st} Twenty	Transient	Dynamic	
Numerical ($n = 2$)	7	15	0	0	57.85
Numerical ($n = 20$)	-	-	0	0	72.36
Fuzzy-Set (Constant)	4	9	0	0	42.89
Fuzzy-Set (Linear)	3	6	0	0	42.90
Fuzzy-Set (Exponential)	1	3	0	0	42.86
Fuzzy-Set (Sigmoid)	0	2	0	0	42.81

Table 8.6: Results for full NGC 93 Machine - 718 Busbar Network

Chapter 9

Conclusions

A new security assessment algorithm has been applied to a pre-existing real-time electro-mechanical power system simulator at the University of Bath. This has required a number of modifications to be made to this simulator in order to accurately model the impact of credible disturbances on several test networks. An artificial intelligence technique has been used for contingency analysis, stability assessment and any alarm processing that may be required during these disturbances. The results of this research are now being used with a subsequent research project into dynamic security assessment.

An expert system approach based on fuzzy set notation has been employed for this research. This has the distinct advantage of allowing a "pseudo" operator to make judgemental decisions on the operating condition of the power system during each contingency analysis period.

Two different computer hardware platforms have been used for the development of this research. These are namely a Microway Number Smasher-860 accelerator card based in a 33MHz IBM PC/AT-386 clone and a Silicon Graphics INDIGO with a 100MHz R4000 RISC processor. Results for both of these architectures are the same, although, as expected, the former was, on average, 2.5 times slower than the latter per contingency evaluation.

A number of different sized study networks were used to test the algorithms developed during the period of this research. A 4 machine and 6 busbar model was used as the development base for this work, since this is a reduction of a full NGC network study and includes a pump-storage generation site, as well as the more conventional thermal plant. A "larger" reduced model containing 20 machines and 100 network nodes was also used as a test bed. Naturally, the number of possible contingencies increased which showed a variety of stability problems. Two scenarios were set up for both of these studies, involving a base case and a more stressed condition, which led to more transient and dynamic/steady state stability violations. These will be described further in this chapter in a later section. The algorithm was also applied to the internationally recognised IEEE 57 busbar test network. This contains 7 generating groups, 3 of which act as synchronous compensators. This network was modified slightly to the American Electric Power Corporation (AEP) standard to include a number of double transmission circuits. The last system model to be used, was that employed by National Grid Company (NGC) in their load flow and stability assessment studies. This contains 93 generators and 718 network nodes, ranging from 400KV to 66KV. A number of double transmission circuit outages were highlighted by off-line studies at NGC. These were tested by the fuzzy security assessor at the University of Bath and ranked effectively equal to the NGC results.

9.1 Contingency Analysis

Code was developed and incorporated into the main body of the simulator PowSim in order to read a contingency database and apply and evaluate each of the disturbances in this database.

The contingency database for each of the networks, mentioned above, included

single, double and triple transmission circuit outages, 3-phase busbar faults, network load and group generation losses for all lines, busbars and groups in the system model. Each database defines the screening and analysis periods for contingency evaluation, as well as an additional time interval for dynamic stability assessment. The fault duration for the 3-phase busbar loss is also included and can be specified by the user in the database. Loss of load and generation were handled by simply removing the sink or source, respectively, from the network. Line contingencies were more complicated and involved applying faults of different durations to the sending and receiving ends of the line (depending on which end is to tripped first) and manipulating the fault impedances to ground on each end node during these durations to mimic, in essence, a form of distance protection.

Once all the contingencies have been applied, additional code was used to order each of them in a ranked list according to their relative severities, i.e. with the most severe at the top. Performance indices were produced by fuzzy set based evaluations on busbar voltage magnitudes, line MVA flows, generator group MVA outputs and reactive power injections from these groups into the network. Each of these quantities calculated by the main loop of PowSim, was normalised with respect to its appropriate rating, for all the lines, busbars and groups in the model network, and categorised into one of a number of fuzzy sets or linguistic variables, according to user-defined limits, for each contingency.

During the development of this contingency analysis algorithm, numerous fuzzy set classifications were used, ranging from three to ten. The former proved to be computationally less demanding than the latter, although a significant decrease in accuracy was observed. In previous work [20, 21, 41], five fuzzy linguistic descriptions have been used, which, for this research, also proved adequate. This was because the accuracy was comparable to the higher order fuzzy set method without

the calculation overhead required to consequently evaluate ten linguistic variables. As in [41], a triangular membership function representation of these fuzzy sets was used. Although other representations have been previously devised, such as normal distribution curves and trapezium approaches, the triangular method is a good approximation to these and has the added advantage of less computational demand for the final defuzzification procedure.

Several weighting functions were implemented which bias this representation of the membership function. Results have been presented for four weighting functions. These are namely constant, linear, exponential [41] and sigmoid. More emphasis is, hence, placed on the middle to high range of the linguistic variables. This was because the effect of contingent quantities falling into this region is of more significant interest than that of the low to middle range.

At the end of each simulation time step, fuzzy set manipulations were used, namely the sum-product rule, in order to calculate the overall system performance index per contingency for each of the quantities mentioned above. This means that when more than one contingent quantity fell into a particular fuzzy set, the membership function of that set would be modified to illustrate this. At the end of each time step the profile of the membership functions were no longer defined by their initial weighting functions and looked more hap-hazard. The area under each of the linguistic variables was calculated to give the total area under all of the triangles. Via a binary search method, the centre of gravity of this area was determined which yielded the total system performance index for that contingent quantity. These were summed together for all quantities analysed to give the total system severity index for that particular contingency.

Two numerical approaches were also used, again with different "weightings" to

show the effect of masking errors. A high order numerical performance index algorithm was employed as the "benchmark" for the other approaches, since this has been proved to be effectively 100% accurate. As the weighting function of the fuzzy set methods became more pronounced, so the accuracy of the solution increased, until a level was reached, as with the sigmoid function, where very few differences were observed between it and the benchmark. Although the solution times per contingency evaluation for the fuzzy set methods and the lower order numerical algorithm were comparable for small systems, the speed-up advantage that can be achieved for larger networks as compared to the benchmark was considerable and, was, on average, approximately 40% for the fuzzy set approaches. This was due to the relative lack of mathematical calculation needed to evaluate each contingency when compared to the benchmark.

9.2 Stability Assessment

During the application of the contingency database for the network models, mentioned previously, the simulator showed a number of stability violations. These included both transient and dynamic/steady state effects.

Transient instabilities were detected by a fuzzy algorithm which, as for the contingency analysis code, categorised a number of quantities during a contingency application into one of four fuzzy sets. The quantities, in this case, were machine rotor angle, kinetic energy and rotor acceleration.

A numerical approach was also employed which simply monitored the time domain solution. This latter method was used as a benchmark for the new fuzzy algorithm.

There were no misclassifications by the new approach when compared to this

benchmark, which showed a 25% computational speed-up advantage. This was because, once potential instability had been detected by the fuzzy algorithm, subsequent contingency analysis was stopped for any further evaluation. This was also true for the time domain solution method but, since this approach is not very good at predicting instability, the solution had to wait for a pole-slip to actually occur.

From the results obtained for the two reduced study networks, i.e. the 4 machine and 6 busbar and the 20 machine and 100 busbar models respectively, it was observed that the number of transiently unstable contingencies increased significantly from the base case to the new stressed condition. This is, of course, quite understandable. However, in these circumstances, the time domain solution took appreciably longer to detect transient instability. This was because, for most of these cases, oscillations built up over a few seconds in a "dynamic stability" mode. The fuzzy algorithm detected these within a second, displaying a 52% speed-up advantage over the benchmark.

During these stressed conditions, a number of dynamic instability cases were highlighted. Again a fuzzy algorithm was used, which categorised machine rotor oscillations according to their amplitude against a threshold value into one of three fuzzy sets. A time domain solution was used as the benchmark for this new approach.

As before, there were no misclassifications by the fuzzy method with an approximate 10% computational speed-up calculated. It was interesting to observe that some of these dynamically unstable contingencies were either sustained rotor oscillations or the amplitude of these oscillations grew over the steady state stability analysis period specified by the user in the contingency database. The latter

conditions either reached a level and remained sustained at this consistent position or continued to increase until synchronism was lost from the rest of the system. This type of solution was preferred over the more traditional eigenvalue analysis, since for larger systems, the fuzzy approach has proved to be computationally less demanding.

9.3 Alarm Processing

Although there was no computational speed-up advantages that could be gained from the addition of an alarm processor, it was thought that a list of network alarms for each contingency would be useful for an operator to track the system state during the disturbance period. Hence an alarm handling algorithm was developed to help reduce the amount of information that the user would otherwise have to process.

It can be seen from Appendices B and C at the end of this thesis that the full alarm list for a single stable contingency can flow onto a number of pages. This is just emphasised by a contingency which is transiently or dynamically unstable.

Two reductions were, therefore, introduced. The first is a general summary listing the number of alarms that were detected around the network and grouped into categories for each contingency. The second is, essentially, very similar, except that the number of alarms are grouped in the particular geographical area in which they occurred. These summaries, however, ultimately depend on what information the operator would need to formulate a set of corrective and/or preventative actions to alleviate some of the more serious problems.

Future developments of this research include modifications to network load representations, protection modelling and a more detailed and refined dynamic stability detection algorithm. Coupled to these, a monitor for voltage stability and proximity to voltage collapse indicator could be developed, as well as a user friendly man-machine interface. The speed-up advantages have been highlighted for a fuzzy-set method over a numerical based algorithm, without a detrimental effect on accuracy (or the simulator PowSim falling out of real-time). However, with the introduction of the distributed parallel processing architecture, mentioned in Section 6.4, analysis of the database for the 20 machine and 100 busbar model, for example, should take considerably less time. The next chapter will discuss these future developments in more detail.

Chapter 10

Suggestions for Further Work

10.1 Protection Modelling

Although a protection scheme has been added to the simulator PowSim, it is very simplistic in its approach. The way in which the relay and circuit breaker operations have been modelled is, in essence, crude and involves simply removing the line from the network topology. Overcurrent protection systems are widely used in distribution networks and as a back-up in transmission systems, even though the latter is gradually being phased out. This basic approach is often applied to generators, transformers and feeders. Theoretically, the fundamental drawback of this type of scheme is that for correct fault discrimination to be obtained, the times of operation close to a supply point can become large.

The short-comings of graded overcurrent relay protection has led, in reality, to the widespread use of distance protection [189]. With the rapid development of interconnected high voltage power systems to ensure continuity of supply and good voltage regulation, the problems of combining fast fault clearance times with power system control have been the areas of many years of research. The final solution is based on the distance between any point on the line and the fault is proportional to the ratio of voltage and current at that point. The protection relays that are responsive to impedance, reactance or admittance (based on the

widely published *mho* characteristics) are often used. Distance protection, when considered as a non-unit scheme (effectively standalone) is of the high speed class and provides both primary and back-up facilities in a single system. It can be modified to a unit scheme (with the use of a signalling channel) and is suited for high speed auto-reclosing for the protection of important transmission lines.

Much of the ground work has been established with the introduction of the "new" line contingency application routine. Modelling the mho circle characteristic for the protection relays will require additional research. It can, hence, be used to establish the new operating state and topology of the system model after critical contingencies.

10.2 Load Modelling

As discussed in Chapter 3, voltage stability is becoming of increasing importance and can be influenced by a number of factors such as network disturbances, the effect of load tap changing transformers and load characteristics at low voltages.

At present, substation loads are modelled by PowSim as constant impedances, which are effectively a composite load consisting of industrial and domestic consumers. In reality, this composition includes induction and synchronous motors, lighting and heating [79]. Lighting and heating can be labelled as static, since the former is independent of frequency and consumes no reactive power, whilst the latter maintains constant resistance with respect to voltage change. The power consumed by synchronous motors is approximately constant, where for a given excitation, VArs change in a leading direction with a reduction in voltage. Modelling of P-V and Q-V characteristics for both synchronous and induction motors were developed by Stagg [171].

The real world P-V and Q-V characteristics of these complete composite loads are of primary interest and very few results have been published. This is, of course, due to consumer objection to such tests being carried out and the difficulty in determining the degree to which motors are loaded. This, in essence, affects the shape of the resultant P-V and Q-V characteristics. It has been suggested that a good approximation is to represent the load as a constant current device for voltage stability studies. It should also be noted that voltage changes often occur with a change in system frequency, so that frequency dependent load characteristics should also be modelled in the future.

10.3 Transformers and FACTS Devices

In addition to the modifications to the modelling of loads, the effect of load tap changing transformers, LTC's, could also be taken into account. PowSim represents both generator and line transformers as devices which typically are set at the nominal tap position of 1 p.u. These have to be altered manually on-line by the user before any change takes place.

Most of the transformers on the U.K. National Grid system have automatic tap changers. These incrementally tap up or down with respect to voltage and frequency within a specified set of limits. A typical range is from 0.8 to 1.2 p.u. with 20 taps existing within these limits. For an accurate simulation of how a power system would theoretically behave during network disturbance conditions, these load tap changing transformers should be modelled and incorporated as part of the simulator PowSim.

Once these transformers have reached their respective upper or lower tap limits, naturally no further change can take place. This, as discussed by the literature

in Section 3.2.4, is another of the important introductions that would need to be made for voltage stability studies. Of course, this naturally has a beneficial knock-on effect for transient and dynamic/steady state stability analyses during contingency evaluation.

The National Grid system also incorporates a number of voltage control devices. These include quadrature boosters and complex static voltage compensators or SVC's. The area of flexible a.c. transmission semi-conductor schemes (FACTS) is also becoming of increasing interest which may, in future, be used to control the devices mentioned above. Therefore, in order to keep up with these new techniques, models may have to be developed.

10.4 Stability Detection Algorithms

Coupled with the two previous sections are the extensions to dynamic and voltage stability analysis algorithms. At present, a crude fuzzy set approach based on a time domain solution has been used for the former. Eigenvalue analysis has been found to be time consuming for large systems. There is an added disadvantage that some networks, particularly the reduced systems, have complex eigenvalues very near to the "imaginary" axis in the steady state operating condition. This can, of course, give a false, albeit conservative, estimate of the system stability. The fuzzy set method has proved to be less computationally expensive, although a quicker solution should be sought. Work is already progressing using an enhancement to the NGC's time constant method [190].

With the introduction of voltage and frequency dependent loads and automatic tap changing transformers, a new avenue is opened for voltage stability studies. Cascaded tripping during a network disturbance, using the improved protection

algorithm, could lead to system islanding or even total system collapse. Hence a voltage stability monitor could be developed, which estimates the proximity to voltage collapse. This could be incorporated as part of the on-line security assessor.

10.5 Fuzzy Set Enhancements

As discussed in Chapter 7, the fuzzy set membership function representation of the five linguistic variables *Very Small*, *Small*, *Medium*, *Large* and *Very Large* was based around a triangular form. Although this is a good approximation to a normal distribution curve, obvious assumptions have been made. Parameters describing a curve such as this, could be determined to ascertain whether the triangular form is too approximate.

In Chapter 8, results were presented for four different weighting functions of these membership function representations. The sigmoid approach proved to be the most accurate when compared to the benchmark. Fine tuning of the parameters for these representations could be made to enhance the results from the contingency ranking to either directly mimic the benchmark or the operator's intuition/experience. Although the width parameter of the medium triangle, for example, was enlarged, the noticeable differences were negligible. However, by moving the peak values up or down the sigmoid profile could yield more prominent results.

A more efficient algorithm could be developed for the defuzzification procedure to give the over all system performance index for each contingent quantity. The binary search method to determine the centre of gravity is accurate, even though it can be computationally expensive, depending on the size and operating condition

of the network.

Static quantities based on busbar voltage magnitudes, line MVA flows, generator group MVA outputs and MVAr injections have been used as the input variables to the contingency analysis routines. Rates of change of these quantities could be used as additional inputs, although this would ultimately be memory intensive (storage of previous values with respect to time). Other variables could also be used such as the MVA flows across critical boundaries. For example, National Grid Company have a set of import and export interface flows, such as the north to south flow limits. These are, however, specific to the particular network being modelled.

10.6 Parallel Versions

This research has been carried out a single processor. This was fine as a development tool but, for large system models and hence contingency databases, obvious drawbacks were observed. A new computing architecture has recently been developed and installed in the laboratory at the University of Bath which acts as a distributed processing network, as described in Section 6.4.

Work has already started on research into a dynamic security assessor, where analytical and numeric techniques have been used to assess the security of the 20 machine and 100 busbar system model when subjected to 854 contingencies. These were transiently analysed in a period of approximately 5 minutes. The Silicon Graphics INDIGO acted as a network server with two IBM PC/AT 486 clones as additional "workers". This cannot really be compared to the timing results obtained for this research, since dynamic instability was not catered for.

It would be interesting to modify the code so that the fuzzy set approaches to contingency analysis and stability assessment could be implemented to ascertain how quickly the results could be produced.

10.7 Man-Machine Interface

Although previous research has been conducted into providing a user-friendly graphics interface between the operator and the simulator [175], no further work has been done in this area. The results from the fuzzy set work has revealed that the output of the security assessor would certainly benefit from such a man-machine interface. X Windows has the capability to display, through a mouse-driven menu system, all three of the alarm specific output files. These are, at present, written to the hardware's hard disk.

An extension to the interface set up by Ng [175] would be useful when applying specific contingencies which are relevant to the particular system operating condition. At present, a number of command lines would need to be typed at the simulator's interactive prompt. This would be a little time consuming depending on whether the operator was under pressure or how many contingencies were to be analysed.

As with all graphics interfaces, a mouse driven method would have to be kept clear, concise and almost simplistic in its design. A trade-off would otherwise be needed, since the operator may in fact spend more time setting up the specific contingency database through a mouse driven action, than if it was to be typed in manually.

References

[1] ELGERD, O.I. : *Electric Energy Systems Theory : An Introduction.* McGraw-Hill, Inc., 1971.

[2] ANDERSON, P.M. AND FOUAD, A.A. : *Power System Control and Stability.* Iowa State University Press, USA, 1977.

[3] STERLING, M.J.H. : *Power System Control.* Peter Peregrinus Ltd, on behalf of IEE (Control Engineering Series), 1978.

[4] NEUENSWANDER, J.R. : *Modern Power Systems.* InterText Book Company, 1973.

[5] DY LIACCO, T.E. : "Real-Time Computer Control of Power Systems", in *Proceedings of the IEEE*, vol. 62, no. 7, pp. 884–891, 1974.

[6] SAVULESCU, S.C., ED. : *Computerised Operation of Power Systems.* Elsevier Scientific Publishing Company, 1976.

[7] STOTT, B. : "Review of Load Flow Calculation Methods", in *Proceedings of the IEEE*, vol. 62, no. 7, pp. 916–929, 1974.

[8] DOPAZO, J.R., KLITIN, O.A., AND SASSON, A.M. : "Stochastic Load Flows", in *IEEE Transactions on Power Apparatus and Systems*, vol. 94, no. 2, pp. 299–309, 1975.

[9] STOTT, B. AND ALSAC, O. : "Fast Decoupled Load Flow", in *IEEE Transactions on Power Apparatus and Systems*, vol. 94, no. 2, pp. 859–869, 1974.

[10] CHRISTIE, R.D., TALUKDAR, S.N., AND NIXON, J.C. : "CQR : A Hybrid Expert System for Security Assessment", in *IEEE Transactions on Power Systems*, vol. 5, no. 4, pp. 1503–1509, 1990.

[11] KERONEN, J.J. : "An Expert System Prototype for Event Diagnosis and Real-Time Operation Planning in Power System Control", in *IEEE Transactions on Power Systems*, vol. 4, no. 2, pp. 544–550, 1989.

[12] KALRA, P.K. AND MATHUR, R.M. : "Investigations for Developing Expert Systems for Power System Control", in *Electric Machines and Power Systems*, vol. 13, no. 4, pp. 265–274, 1987.

[13] JOURDIN, P., VINTACHE, P., HEILBRANN, B., CARTIGNIES, E., MILLOT, P., AND LAGRANGE, V. : "Description of an On-Line Decision Aid Tool for Generation-Load Balance Control", in *IEEE Transactions on Power Systems*, vol. 9, no. 1, pp. 241–247, 1994.

[14] VALIQUETTE, V., TORRES, G.L., AND MUKHEDKAN, D. : "An Expert System Based Diagnosis and Adviser Tool for Teaching Power System Operation Emergency Control Strategies", in *IEEE Transactions on Power Systems*, vol. 6, no. 3, pp. 1315–1322, 1991.

[15] SAKAGUSHI, T., TANAKA, H., VENISHI, K., GOTOH, T., AND SEKINE, Y. : "Prospects of Expert Systems in Power System Operation", in *Int. J. Electric Power and Energy Systems*, vol. 10, no. 2, pp. 71–82, 1988.

[16] BALUE, N.J., ADAPA, R., CAULEY, G., LAUBY, M.G., AND MARATUKULAM, D.J. : "Review of Expert Systems in Bulk Power System Planning and Operation", in *Proceedings of the IEEE*, vol. 80, no. 5, pp. 727–731, 1992.

[17] CHUI, D. AND LAUGHTON, M.A. : "Power System Control Using Fuzzy Reasoning", in 10^{th} *Power Systems Computation Conference in Graz, Austria*, pp. 345–350, 1990.

[18] AKIMOTO, Y., TANAKA, H., YOSHIZAWA, J., KLAPPER, D.B., PRICE, W.W., AND WIRAGU, K.A. : "Application of Expert Systems to Transient Stability Studies", in 2^{nd} *Symposium on Expert Systems Application to Power Systems*, pp. 211–217, 1989.

[19] RIBBENS-PAVELLA, M., WEHENKEL, L., AKELLA, V.B., EUXIBIE, E., TROKIGNON, M., DUCHAMP, A., AND HEILBRONN, B. : "Multicontingency Decision Trees for Transient Stability Assessment", in 11^{th} *Power Systems Computation Conference in Avignon, France*, pp. 113–120, 1993.

[20] MATOS, M.A., PEÇAS LOPES, J.A., AND MACIEL BARBOSA, F.P. : "Fuzzy Classification for On-Line Transient Stability Assessment of Electric Power Systems", in 10^{th} *Power Systems Computation Conference in Graz, Austria*, pp. 865–871, 1990.

[21] HSU, Y.Y. AND SU, C.C. : "A Rule-Based Expert System for Steady State Stability Analysis", in *IEEE Transactions on Power Systems*, vol. 6, no. 2, pp. 771–777, 1991.

[22] WOLLENBERG, B.F. : "Feasibility Study for an Energy Management System Intelligent Alarm Processor", in *IEEE Transactions on Power Systems*, vol. 1, no. 2, pp. 241–246, 1986.

[23] MUNNEKE, M. AND DILLON, T.S. : "Implementation of an Alarm Processing Expert System in a Regional Control Centre", in 10^{th} *Power Systems Computation Conference in Graz, Austria*, pp. 936–943, 1990.

[24] KIRSCHEN, D.S. AND WOLLENBERG, B.F. : "Intelligent Alarm Processing in Power Systems", in *Proceedings of the IEEE*, vol. 80, no. 5, pp. 663–672, 1992.

[25] KHOSLA, R. AND DILLON, T.S. : "Combined Symbolic-Artificial Neural-Net Alarm Processing System", in 11^{th} *Power Systems Computation Conference in Avignon, France*, pp. 259–266, 1993.

[26] EICKHOFF, F., HANDSCHIN, E., AND HOFFMANN, W. : "Knowledge-Based Alarm Handling and Fault Location in Distribution Networks", in *IEEE Transactions on Power Systems*, vol. 7, no. 2, pp. 770–776, 1992.

[27] MCDONALD, J.R., BURT, G.M., AND YOUNG, D.J. : "Alarm Processing and Fault Diagnosis Using Knowledge-Based Systems for Transmission and Distribution Network Control", in *IEEE Transactions in Power Systems*, vol. 7, no. 3, pp. 1292–1298, 1992.

[28] SAKAGUCHI, T. AND MATSUMOTO, K. : "Development of a Knowledge-Based System for Power System Restoration", in *IEEE Transactions on Power Apparatus and Systems*, vol. 102, no. 2, pp. 320–329, 1983.

[29] KIRSCHEN, D.S. AND VOLKMANN, T.L. : "Guiding a Power System Restoration with an Expert System", in *IEEE Transactions on Power Systems*, vol. 6, no. 2, pp. 558–566, 1991.

[30] WANG, S.M., DONG, Z.Z., SUN, Q.H., AND XIA, D.Z. : "A Decision-Support Expert System for Bulk Power System Restoration", in 10^{th} *Power Systems Computation Conference in Graz, Austria*, pp. 966–971, 1990.

[31] FUKUI, S., HORI, S., SIMAKURA, Y., AND INAGAKI, J. : "A Knowledge-Based Approach for the Determination of Restorative Operation Procedures for Bulk Power Systems", in 11^{th} *Power Systems Computation Conference in Avignon, France*, pp. 281–287, 1993.

[32] VADARI, S.V. AND VENKATA, S.S. : "Expert System Load Shedding : A Hybrid Load Shedding Expert System in the Real-Time EMS Environment", in 10^{th} *Power Systems Computation Conference in Graz, Austria*, pp. 929–935, 1990.

[33] ABDULRAHMAN, K.H. AND SHAHIDEHPOUR, S.M. : "A Fuzzy-Based Optimal Reactive Power Control", in *IEEE Transaction on Power Systems*, vol. 8, no. 2, pp. 662–670, 1993.

[34] YOKOYAMA, R., NIRMURA, T., AND NAKANISHI, Y. : "A Co-ordinated Control of Voltage and Reactive Power by Heuristic Modelling and Approximate Reasoning", in *IEEE Transactions on Power Systems*, vol. 8, no. 2, pp. 636–645, 1993.

[35] TOMSOVIC, K. : "A Fuzzy Linear Programming Approach to the Reactive Power Voltage Control Problem", in *IEEE Transactions on Power Systems*, vol. 7, no. 1, pp. 287–295, 1992.

[36] SALAMA, M.M.A. AND CHIKHANI, A.Y. : "An Expert System for Reactive Power Control of a Distribution System", in *IEEE Transaction on Power Delivery*, vol. 7, no. 2, pp. 940–945, 1992.

[37] CHENG, S.J., MALIK, O.P., AND HOPE, G.S. : "An Expert System for Voltage and Reactive Power Control of a Power System", in *IEEE Transactions on Power Systems*, vol. 3, no. 4, pp. 1449–1455, 1988.

[38] CHRISTIE, R.D. AND TALUKDAR, S.N. : "Expert Systems for On-Line Security Assessment : A Preliminary Design", in *IEEE Transactions on Power Systems*, vol. 3, no. 2, pp. 654–659, 1988.

[39] SOBAJIC, D.J. AND PAO, Y.H. : "An Artificial Intelligence System for Power System Contingency Screening", in *IEEE Transactions on Power Systems*, vol. 3, no. 2, pp. 647–653, 1988.

[40] TALUKDAR, S.N. AND CHRISTIE, R.D. : "An Extended Framework for Security Assessment", in 10^{th} *Power Systems Computation Conference in Graz, Austria*, pp. 880–885, 1990.

[41] HSU, Y.Y. AND KUO, H.C. : "Fuzzy-Set Based Contingency Ranking", in *IEEE Transactions on Power Systems*, vol. 7, no. 3, pp. 1189–1195, 1992.

[42] CAULEY, G., KUMAR, A.B.R., BRANDWAJN, V., AND IPAKCHI, A. : "Artificial Intelligence Applications in On-Line Dynamic Security Assessment", in 11^{th} *Power Systems Computation Conference in Avignon, France*, pp. 881–887, 1993.

[43] SASAKI, H., WATANABE, M., KUBOKAWA, J., YORINO, N., YOKOYAMA, R., OUYANG, Z., AND SHAHIDEHPOUR, S.M. : "A Solution Method of Unit Commitment by Artificial Neural Networks", in *IEEE Transactions on Power Systems*, vol. 7, no. 3, pp. 974–981, 1992.

[44] WONG, K.P. AND DOAN, K. : "Artifical Intelligence Algorithm for Daily Scheduling of Thermal Generators", in *Proceedings of the IEE, Part C - Generation, Transmission and Distribution*, vol. 138, no. 6, pp. 518–534, 1991.

[45] MAKHITARI, S., SINGH, J., AND WOLLENBERG, B.F. : "A Unit Commitment Expert System", in *IEEE Transactions on Power Systems*, vol. 3, pp. 272–277, 1988.

[46] LIN, C.E., HUANG, C.J., HUANG, C.L., LIANG, C.C., AND LEE, S.Y. : "An Expert System for Generator Maintenance Scheduling Using Operation Index", in *IEEE Transactions on Power Systems*, vol. 7, no. 3, pp. 1141–1148, 1992.

[47] HSU, Y.Y. AND YANG, C.C. : "Design of Artificial Neural Networks for Short Term Load Forecasting.1 : Self-Organising Feature Maps for Day Type Identification", in *Proceedings of the IEE, Part C - Generation, Transmission and Distribution*, vol. 138, no. 5, pp. 407–413, 1991.

[48] HSU, Y.Y. AND YANG, C.C. : "Design of Artificial Neural Networks for Short Term Load Forecasting.2 : Multilayer Feedforward Networks for Peak Load and Valley Load Forecasting", in *Proceedings of the IEE, Part C - Generation, Transmission and Distribution*, vol. 5, no. 2, pp. 414–418, 1991.

[49] ZADEH, L.A. : "Fuzzy Sets", in *Information and Control*, vol. 8, pp. 338–353, 1965.

[50] ZADEH, L.A. : "Outline of a New Approach to the Analysis of Complex Systems and Decision Processes", in *IEEE Transactions on Systems, Man and Cybernetics*, vol. 3, no. 1, pp. 28–44, 1973.

[51] ZIMMERMANN, H.J. : *Fuzzy Set Theory and its Applications.* Kluwer Academic Publishers, 2^{nd} ed., 1991.

[52] BALU, N.J., BERTRAM, T., BOSE, A., BRANDWAJN, V., CAULEY, G., CURTICE, D., FOUAD, A.A., FINK, L., LAUBY, M.G., WOLLENBERG, B.F., AND WRUBEL, J.N. : "On-Line Power System Security Analysis", in *Proceedings of the IEEE*, vol. 80, no. 2, pp. 262–281, 1992.

[53] HALPIN, T.F., FISCHL, R., AND FINK, R. : "Analysis of Automatic Contingency Selection Algorithms", in *IEEE Transactions on Power Apparatus and Systems*, vol. 103, no. 5, pp. 938–945, 1984.

[54] SCHÄFER, K.F. AND VERSTEGE, J.F. : "Adaptive Procedure for Masking Effect Compensation in Contingency Selection Algorithms", in *IEEE Transactions on Power Systems*, vol. 5, no. 2, pp. 539–546, 1990.

[55] EJEBE, G.C. AND WOLLENBERG, B.F. : "Automatic Contingency Selection", in *IEEE Transactions on Power Apparatus and Systems*, vol. 98, no. 1, pp. 97–104, 1979.

[56] MIKOLINNAS, T.A. AND WOLLENBERG, B.F. : "An Advanced Contingency Selection Algorithm", in *IEEE Transactions on Power Apparatus and Systems*, vol. 100, no. 2, pp. 608–615, 1981.

[57] IRISARRI, G.D., SASSON, A.M. AND LEVNER, D. : "Automatic Contingency Selection for On-Line Security Analysis - Real-Time Tests", in *IEEE Transactions on Power Apparatus and Systems*, vol. 98, no. 5, pp. 1552–1557, 1979.

[58] IRISARRI, G.D. AND SASSON, A.M. : "An Automatic Contingency Selection Method for On-Line Security Analysis", in *IEEE Transactions on Power Apparatus and Systems*, vol. 100, no. 4, pp. 1838–1843, 1981.

[59] ALBUYEH, F., BOSE, A., AND HEATH, B.A. : "Reactive Power Considerations in Automatic Contingency Selection", in *IEEE Transactions on Power Apparatus and Systems*, vol. 101, no. 1, pp. 107–112, 1982.

[60] ENNS, M.K., QUADA, J.J., AND SACKETT, B. : "Fast Linear Contingency Analysis", in *IEEE Transactions on Power Apparatus and Systems*, vol. 101, no. 4, pp. 783–791, 1982.

[61] VEMURI, S. AND USHER, R.E. : "On-Line Automatic Contingency Selection Algorithms", in *IEEE Transactions on Power Apparatus and Systems*, vol. 102, no. 2, pp. 346–354, 1983.

[62] WASLEY, R.G. AND DANESHDOOST, M. : "Identification and Ranking of Critical Contingencies in Dependent Variable Space", in *IEEE Transactions on Power Apparatus and Systems*, vol. 102, no. 4, pp. 881–892, 1983.

[63] LAUBY, M.G., MIKOLINNAS, T.A., AND REPPEN, N.D. : "Contingency Selection of Branch Outages Causing Voltage Problems", in *IEEE Transaction on Power Apparatus and Systems*, vol. 102, no. 12, pp. 3899–3902, 1983.

[64] DABBAGHCHI, I. AND IRISARRI, G.D. : "AEP Automatic Contingency Selector : Branch Outage Impacts on Load Bus Voltage Profile", in *IEEE Transactions on Power Systems*, vol. 1, no. 2, pp. 37–44, 1986.

[65] CHEN, Y. AND BOSE, A. : "Direct Ranking for Voltage Contingency Selection", in *IEEE Transactions on Power Systems*, vol. 4, no. 4, pp. 1335–1341, 1989.

[66] EJEBE, G.C., VAN MEETEREN, H.P., AND WOLLENBERG, B.F. : "Fast Contingency Screening and Evaluation for Voltage Security Analysis", in *IEEE Transactions on Power Systems*, vol. 3, no. 4, pp. 1582–1588, 1988.

[67] BRANDWAJN, V. AND LAUBY, M.G. : "Complete Bounding Method for AC Contingency Screening", in *IEEE Transactions on Power Systems*, vol. 4, no. 2, pp. 724–728, 1989.

[68] HADJSAID, N., BENAHMED, M., FANDINO, J., SABONNADIERE, J.C., AND NERIN, G. : "Fast Contingency Screening for Voltage-Reactive Considerations in Security Analysis", in *IEEE Transactions on Power Systems*, vol. 8, no. 1, pp. 144–150, 1993.

[69] EKWUE, A.O. AND LAING, W.D. : "Critical Evaluation of Voltage-Based Contingency Selection Algorithms for On-Line Applications", in 10^{th} *Power Systems Computation Conference in Graz, Austria*, pp. 835–839, 1990.

[70] EKWUE, A.O. AND SHORT, M.J. : "Improved Decoupled Contingency Selection Algorithms", in *Electric Power Systems Research*, pp. 215–223, 1991.

[71] EKWUE, A.O. : "On the Ranking of Contingencies for On-Line Applications", in *Electric Power Systems Research*, pp. 207–212, 1990.

[72] CHANG, C.C. AND HSU, Y.Y. : "A New Approach to Dynamic Contingency Selection", in *IEEE Transactions on Power Systems*, vol. 5, no. 4, pp. 1524–1528, 1990.

[73] EL-KADY, M.A., FOUAD, A.A., LIU, C.C., AND VENKATARAMAN, S., "Use of Expert Systems in Dynamic Security Assessment of Power Systems", in 10^{th} *Power Systems Computation Conference in Graz, Austria*, pp. 913–920, 1990.

[74] SOBAJIC, D.J. AND PAO, Y.H. : "Artificial Neural-Net Based Dynamic Security Assessment for Electric Power Systems", in *IEEE Transactions on Power Systems*, vol. 4, no. 1, pp. 220–228, 1989.

[75] FISCHL, R., KAM, M., CHOW, J.C., AND YAN, H.H. : "On the Design of Neural Networks for Detecting Limiting Contingencies in Power System Operation", in 10^{th} *Power Systems Computation Conference in Graz, Austria*, pp. 887–894, 1990.

[76] EL-SHARKAWI, M.A., MARKS, R.J., DAMBORG, M.J., ATLAS, L.E., COHN, D.A., AND AGGOUNE, M. : "Artificial Neural Networks as Operator Aid for On-Line Static Security Assessment of Power Systems", in 10^{th} *Power Systems Computation Conference in Graz, Austria*, pp. 895–901, 1990.

[77] PAO, Y.H. AND SOBAJIC, D.J. : "Combined Use of Unsupervised and Supervised Learning for Dynamic Security Assessment", in *IEEE Transactions on Power Systems*, vol. 6, no. 1, pp. 278–284, 1991.

[78] FOUAD, A.A., ZHOU, Q., AND DAVIDSON, J. : "Security/Vulnerability Assessment of a Stability-Limited Power System Using Artificial Neural Networks", in 11^{th} *Power Systems Computation Conference in Avignon, France*, pp. 487–493, 1993.

[79] WEEDY, B.M. : *Electric Power Systems.* John Wiley and Sons, 3^{rd} ed., 1987.

[80] KIMBARK, E.W. : *Power System Stability*, vol. 1. Wiley, New York, 1948.

[81] KIMBARK, E.W. : *Power System Stability*, vol. 2. Wiley, New York, 1948.

[82] KIMBARK, E.W. : *Power System Stability*, vol. 3. Wiley, New York, 1948.

[83] CIGRE TASK FORCE 38.02.09, "Assessment of Practical Fast Transient Stability Methods — State of the Art Report", Tech. Rep., CIGRE, 1992.

[84] FOUAD, A.A. AND VITTAL, V. : "The Transient Energy Function Method", in *Int. J. Electric Power and Energy Systems*, pp. 233–246, 1988.

[85] FOUAD, A.A. AND VITTAL, V. : *Power System Transient Stability Analysis Using the Transeint Energy Function.* Prentice-Hall, New Jersey, 1992.

[86] FOUAD, A.A., VITTAL, V., AND OH, T.K. : "Critical Energy for Direct Transient Stability Assessment of a Multi-Machine Power System", in *IEEE Transactions on Power Apparatus and Systems*, vol. 103, no. 8, pp. 2199–2206, 1984.

[87] FOUAD, A.A., STANTON, S.E., MAMANDUR, K.R.C., AND KRUEMPEL, K.C. : "Contingency Analysis Using the Transient Energy Function", in *IEEE Transactions on Power Apparatus and Systems*, vol. 101, no. 4, pp. 757–765, 1982.

[88] XUE, Y., VAN CUTSEM, TH., AND RIBBENS-PAVELLA, M. : "A Simple Direct Method for Fast Transient Stability Assessment of Large Power Systems", in *IEEE Transactions on Power Systems*, vol. 3, no. 2, pp. 400–412, 1988.

[89] KAKIMOTO, N., OHNOGI, Y., MATSUDA, H., AND SHIBUYA, H. : "Transient Stability Analysis of Large-Scale Power Systems by Lyapunov's Direct Method", in *IEEE Transactions on Power Apparatus and Systems*, vol. 103, no. 1, pp. 160–167, 1984.

[90] HAKIMMASHHADI, H. AND HEYDT, G.T. : "Fast Transient Security Assessment", in *IEEE Transactions on Power Apparatus and Systems*, vol. 102, no. 12, pp. 3816–3824, 1983.

[91] XUE, Y., VAN CUTSEM, TH., AND RIBBENS-PAVELLA, M. : "Extended Equal-Area Criterion : Justifications, Generalizations, Applications", in *IEEE Transactions on Power Systems*, vol. 4, no. 1, pp. 44–52, 1989.

[92] XUE, Y., WEHENKEL, L., BELHOMME, R., ROUSSEAUX, P., RIBBENS-PAVELLA, M., EUXIBIE, E., HEILBRONN, B., AND LESIGNE, J. : "Extended Equal-Area Criterion Revisited", in *IEEE PES Summer Meeting*, pp. 422–426, 1991.

[93] XUE, Y. AND RIBBENS-PAVELLA, M. : "Extended Equal-Area Criterion : An Analytical Ultra-Fast Method for Transient Stability Assessment and Preventive Control of Power Systems", in *Int. J. Electric Power and Energy Systems*, pp. 131–149, 1989.

[94] LO, K.L. AND HILAL, H. : "Direct Assessment of Power Systems Transient Stability Via Lyapunov Method", in *Proceedings of the* 25^{th} *Universities Power Engineering Conference in Aberdeen, UK*, pp. 227–230, 1990.

[95] ATHAY, T.M., PROCOMORE, R., AND VIRMANI, S. : "A Practical Method for the Direct Analysis of Transient Stability", in *IEEE Transactions on Power Apparatus and Systems*, vol. 98, no. 2, pp. 573–584, 1979.

[96] TAVORA, C.J. AND SMITH, O.J.M. : "Equilibrium Analysis of Power Systems", in *IEEE Transactions of Power Apparatus and Systems*, vol. 91, no. 3, pp. 1138–1145, 1972.

[97] RAHIMI, F.A., LAUBY, M.G., WRUBEL, J.N., AND LEE, K.L. : "Evaluation of the Transient Energy Function Method for On-Line Dynamic Security Analysis", in *IEEE Transactions on Power Systems*, vol. 8, no. 2, pp. 497–503, 1993.

[98] MARIA, G.A., TANG, C., AND KIM, J. : "Hybrid Transient Stability Analysis", in *IEEE Transactions on Power Systems*, vol. 5, no. 2, pp. 384–389, 1990.

[99] BERRY, T., DALE, L.A., DANIELS, A.R. AND DUNN, R.W. :, "Real-Time Modelling of Multi-Machine Power Systems", in *Proceedings of the IEE, Part C - Generation, Transmission and Distribution*, vol. 140, no. 4, pp. 241–248, 1993.

[100] CHAN, K.W. AND DANIELS, A.R. AND DUNN, R.W. AND BERRY, T. : "A Partitioning Algorithm for Parallel Processing of Large Power System Network Equations", in *IEE* 2^{nd} *International Conference in Power System Control, Operation and Management, Hong Kong*, vol. 2, no. 34, pp. 893–898, 1993.

[101] HWONG, K. : "Advanced Parallel Processing with Supercomputer Architectures", in *Proceedings of the IEEE*, vol. 75, no. 10, pp. 1348–1379, 1987.

[102] LIU, S., WANG, X.P., AND YU, Q.Z. : "Hybrid Transient Stability Analysis Using a Structure Preserving Model", in 11^{th} *Power Systems Computation Conference in Avignon, France*, pp. 89–95, 1993.

[103] DECKER, I.C., FALCAO, D.M., AND KASZKUREWICZ, E. : "Parallel Implementation of Power System Dynamic Simulation Methodology Using the Conjugate Gradient Method", in *IEEE Transactions on Power Systems*, vol. 7, no. 1, pp. 458–465, 1992.

[104] LA SCALA, M., BRUCOLI, M., TORELLI, F., AND TROVATO, M. : "A Gauss-Jacob-Block-Newton Method for Parallel Transient Stability Analysis", in *IEEE Transactions on Power Systems*, vol. 5, no. 4, pp. 1168–1177, 1990.

[105] YAMASHIRO, S., KOIKE, T., AND EL-ABIAD, A.H. : "Fast Transient Security Assessment and Enhancement of Electric Power Systems Using Pattern Recognition", in 8^{th} *Power Systems Computation Conference in Helsinki, Finland*, pp. 891–897, 1984.

[106] EDWARDS, A.R. : "Detection of Instability in Power Systems Using Connectionism", Transfer Report from MSc to PhD, University of Bath, School of Electronic & Electrical Engineering, 1994.

[107] MIRANDA, V., FIDALGO, J.N., PEÇAS-LOPES, J.A., AND ALMEIDA, L.B. : "Fast Assessment of Transient Stability Margins by a Neural Network Approach", in 11^{th} *Power Systems Computation Conference in Avignon, France*, pp. 81–88, 1993.

[108] DE MELLO, F.P. AND LASKOWSKI, T.F. : "Concepts of Power System Dynamic Stability", in *IEEE Transactions on Power Apparatus and Systems*, vol. 94, no. 3, pp. 827–833, 1975.

[109] LANGEVIN, M. AND AURIOL, P. : "Load Response to Voltage Variations and Dynamic Stability", in *IEEE Transactions on Power Systems*, vol. 1, no. 4, pp. 112–118, 1986.

[110] TORRE, W.V. AND BUSHNER, R.E. : "A Unique Method of Evaluation of System Damping in Simulations of Large Power Systems", in *IEEE Transactions on Power Systems*, vol. 2, no. 1, pp. 119–122, 1987.

[111] MACHIAS, A.V., SOUFLIS, J.L., AND PAPADIAS, B.C. : "Application of a Deep Level Knowledge Model to Dynamic Behaviour Analysis of Power Systems", in *IEEE Transactions on Systems, Man and Cybernetics*, vol. 20, no. 5, pp. 701–708, 1990.

[112] BURCHETT, R.C. AND HEYDT, G.T. : "Probabilistic Methods for Power System Dynamic Stability Studies", in *IEEE Transactions on Power Apparatus and Systems*, vol. 97, no. 3, pp. 695–702, 1978.

[113] SAITOH, H., TOYODA, J., AND KOBAYASHI, Y. : "A New Index Extracted from Line Flow Fluctuation to Evaluate Power System Damping", in *IEEE Transactions on Power Systems*, vol. 6, no. 4, pp. 1473–1479, 1991.

[114] OBATA, Y., TAKEDA, S., AND SUZUKI, H. : "An Efficient Eigenvalue Estimation Technique for Multi-Machine Power System Dynamic Stability Analysis", in *IEEE Transactions on Power Apparatus and Systems*, vol. 100, no. 1, pp. 259–263, 1981.

[115] RUDNICK, H., HUGHES, F.M., AND BRAMELLER, A. : "Steady State Instability : Simplified Studies in Multi-Machine Power Systems", in *IEEE Transactions on Power Apparatus and Systems*, vol. 102, no. 12, pp. 3859–3866, 1983.

[116] UCHIDA, N. AND NAGAO, T. : "A New Eigen-Analysis Method of Steady State Stability Studies for Large Power Systems : S Matrix Method", in *IEEE Transactions on Power Systems*, vol. 3, no. 2, pp. 706–712, 1988.

[117] PAGOLA, F.L., PÉREZ-ARRIAGA, I.J., AND VERGHESE, G.C. : "On Sensitivities, Residues and Participations : Applications to Oscillatory Stability Analysis and Control", in *IEEE Transactions on Power Systems*, vol. 4, no. 1, pp. 278–285, 1989.

[118] KUNDUR, P., ROGERS, G.J., WONG, D.Y., WANG, L., AND LAUBY, M.G. : "A Comprehensive Computer Program Package for Small Signal Stability Analysis of Power Systems", in *IEEE Transactions on Power Systems*, vol. 5, no. 4, pp. 1076–1083, 1990.

[119] SEMLYEN, A. AND WANG, L. : "Sequential Computation of the Complete Eigen-System for the Study Zone in Small Signal Stability Analysis of Large Power Systems", in *IEEE Transactions on Power Systems*, vol. 3, no. 2, pp. 715–721, 1988.

[120] HSU, Y.Y., SHYUE, S.W., AND SU, C.C. : "Low Frequency Oscillations in Longitudinal Power Systems : Experience with Dynamic Stability of Taiwan Power System", in *IEEE Transactions on Power Systems*, vol. 2, no. 1, pp. 92–98, 1987.

[121] ABE, S., FUKUNAGA, Y., ISONO, A., AND KONDO, B. : "Power System Voltage Stability", in *IEEE Transactions on Power Apparatus and Systems*, vol. 101, no. 10, pp. 3830–3838, 1982.

[122] TAMURA, Y., MORI, H., AND IWAMOTO, S. : "Relationship Between Voltage Instability and Multiple Load Flow Solutions in Electric Power Systems", in *IEEE Transactions on Power Apparatus and Systems*, vol. 102, no. 5, pp. 1115–1123, 1983.

[123] KWATNY, H.G., PASRIJA, A.K., AND BAHAR, L.Y. : "Static Bifurcations in Electric Power Networks : Loss of Steady State Stability and Voltage Collapse", in *IEEE Transactions on Circuits and Systems*, vol. 33, no. 10, pp. 981–991, 1986.

[124] TIRANUCHIT, A., EWERBRING, L.M., DURYEA, R.A., THOMAS, R.J., AND LUK, F.T. : "Towards a Computationally Feasible On-Line Voltage Instability Index", in *IEEE Transactions on Power Systems*, vol. 3, no. 2, pp. 669–675, 1988.

[125] OBADINA, O.O. AND BERG, G.J. : "Determination of Voltage Stability Limit in Multi-Machine Power Systems", in *IEEE Transactions on Power Systems*, vol. 3, no. 4, pp. 1545–1552, 1988.

[126] LÖF, P.A., ANDERSSON, G., AND HILL, D.J. : "Voltage Stability Indices for Stressed Power Systems", in *IEEE Transactions on Power Systems*, vol. 8, pp. 326–332, 1993.

[127] MERCEDE, F.J., CHOW, J.C., YAN, H.H., AND FISCHL, R. : "A Framework to Predict Voltage Collapse in Power Systems", in *IEEE Transactions on Power Systems*, vol. 3, no. 4, pp. 1807–1813, 1988.

[128] FLATABØ, N., OGNEDAL, R., AND CARLSEN, T. : "Voltage Stability Condition in a Power Transmission System Calculated by Sensitivity Methods", in *IEEE Transactions on Power Systems*, vol. 3, no. 1, pp. 1286–1292, 1990.

[129] BEGOVIĆ, M.M. AND PHADKE, A.G. : "Control of Voltage Stability Using Sensitivity Analysis", in *IEEE Transactions on Power Systems*, vol. 7, no. 1, pp. 114–120, 1992.

[130] GAO, B., MORISON, G.K., AND KUNDUR, P. : "Voltage Stability Evaluation Using Modal Analysis", in *IEEE Transactions on Power Systems*, vol. 7, no. 4, pp. 1529–1536, 1992.

[131] MORISON, G.K., GAO, B., AND KUNDUR, P. : "Voltage Stability Analysis Using Static and Dynamic Approaches", in *IEEE Transactions on Power Systems*, vol. 8, no. 3, pp. 1159–1165, 1993.

[132] AMELINK, H., FORTE, A.M., AND GUBERMAN, R.P. : "Dispatcher Alarm and Message Processing", in *IEEE Transactions on Power Systems*, vol. 1, no. 3, pp. 188–194, 1986.

[133] TESCH, D.B., YU, D.C., FU, L.M., AND VAIRAVAN, K. : "A Knowledge-Based Alarm Processor for an Energy Management System", in *IEEE Transactions on Power System*, vol. 5, no. 1, pp. 268–275, 1990.

[134] BIJOCH, R.W., HARRIS, S.H., VOLKMANN, T.L., BANN, J.J., AND WOLLENBERG, B.F. : "Development and Implementation of the NSP Intelligent Alarm Processor", in *IEEE Transactions on Power Systems*, vol. 6, no. 2, pp. 806–812, 1991.

[135] BELL, K.R.W : "Artificial Intelligence and Uncertainty in Power Systems", 1994. Transfer Report from MSc to PhD, University of Bath, School of Electronic & Electrical Engineering, 1994.

[136] STOTT, B., ALSAC, O., AND MONTICELLI, A.J. : "Security Analysis and Optimisation", in *Proceedings of the IEEE*, vol. 75, no. 12, pp. 1623–1644, 1987.

[137] CHANG, S.S.L. AND ZADEH, L.A. : "On Fuzzy Mapping and Control", in *IEEE Transactions on Systems, Man and Cybernetics*, vol. 2, no. 1, pp. 30–34, 1972.

[138] MAMDANI, E.H. AND ASSILIAN, S. : "An Experiment in Linguistic Synthesis with a Fuzzy Logic Controller", in *Int. J. Man-Mach. Stud.* vol. 7, pp. 1–13, 1975.

[139] MAMDANI, E.H. AND KING, P. : "Application of Fuzzy Control Systems to Industrial Processes", in *Automatica*, vol. 13, pp. 235–242, 1977.

[140] LARSEN, P. : "Industrial Applications of Fuzzy Logic Control", in *Int. J. Man-Mach. Stud.* vol. 12, pp. 3–10, 1980.

[141] TONG, R.M. : "A Control Engineering Review of Fuzzy Systems", in *Automatica*, vol. 13, pp. 559–569, 1977.

[142] MAIERS, J. AND SHERIF, Y.S. : "Applications of Fuzzy Set Theory", in *IEEE Transactions on Systems, Man and Cybernetics*, vol. 15, no. 1, pp. 175–189, 1985.

[143] PAPPIS, C.P. AND MAMDANI, E.H. : "A Fuzzy Logic Controller for a Traffic Junction", in *IEEE Transactions on Systems, Man and Cybernetics*, vol. 7, no. 10, pp. 707–717, 1977.

[144] MAMDANI, E.H. : "Application of Fuzzy Logic to Approximate Reasoning Using Linguistic Synthesis", in *IEEE Transactions on Computers*, vol. 26, no. 12, pp. 1182–1191, 1977.

[145] MAMDANI, E.H. AND PROCYK, T. : "A Linguistic Self-Organising Process Controller", in *Automatica*, vol. 15, pp. 15–30, 1979.

[146] TONG, R.M. : "Some Properties of Fuzzy Feedback Systems", in *IEEE Transactions on Systems, Man and Cybernetics*, vol. 10, no. 6, pp. 327–330, 1980.

[147] CUMANI, A. : "On a Possibilistic Approach to the Analysis of Fuzzy Feedback Systems", in *IEEE Transactions on Systems, Man and Cybernetics*, vol. 12, no. 7, pp. 417–422, 1982.

[148] FREELING, A.N.S. : "Fuzzy Sets and Decision Analysis", in *IEEE Transactions on Systems, Man and Cybernetics*, vol. 10, no. 7, pp. 341–354, 1980.

[149] CZOGALA, E. AND PEDRYCZ, W. : "Some Problems Concerning the Construction of Algorithms of Decision Making in Fuzzy Systems", in *Int. J. Man-Mach. Stud.* vol. 15, pp. 201–211, 1981.

[150] MAMDANI, E.H. : "Advances in the Linguistic Synthesis of Fuzzy Controllers", in *Int. J. Man-Mach. Stud.* vol. 8, pp. 669–678, 1976.

[151] BAAS, S.M. AND KWAKERNAAK, H. : "Rating and Ranking of Multiple Aspect Alternatives Using Fuzzy Sets", in *Automatica*, vol. 13, pp. 47–58, 1977.

[152] DUBOIS, D. AND PRADE, H. : "A Procedure for Multiple Aspect Decision Making", in *Int. J. Syst. Sci.* vol. 9, pp. 357–360, 1978.

[153] RUTHERFORD, D.A. AND BLOORE, G.C. : "The Implementation of Fuzzy Algorithms for Control", in *Proceedings of the IEEE*, pp. 572–573, 1976. Proceedings Letter.

[154] MOTOROLA SEMICONDUCTOR APPLICATION NOTE, "Fuzzy Logic and Neuron Chip, Document no. AN1225", Tech. Rep., Motorola Inc., 1993.

[155] MOTOROLA SEMICONDUCTOR APPLICATION NOTE, "Parallel I/O Interface to the Neuron Chip, Document no. AN1208", Tech. Rep., Motorola Inc., 1994.

[156] MOTOROLA SEMICONDUCTOR TECHNICAL DATA, "Neuron Chip Distributed Communications and Control Processors, Document no. MC143150", Tech. Rep., Motorola Inc., 1994.

[157] REINFRANK, M. : "Fuzzy Control Systems : Clear Advantages", *Siemens Review*, pp. 28–32, 1991.

[158] EFSTATHIOU, J. : "Expert Systems, Fuzzy Logic and Rule-Based Control Explained At Last", in *Transactions of the Inst. M. C.* vol. 10, pp. 198–206, 1988.

[159] DUBOIS, D. AND PRADE, H. : *Fuzzy Sets and Systems : Theory and Applications.* Academic Press, New York, 1980.

[160] GIARRATANO, J. AND RILEY, G. : *Expert Systems : Principles and Programming.* PWS-Kent Publishing Company, 1989.

[161] KLIR, G.J. AND FOLGER, T.A. : *Fuzzy Sets, Uncertainty and Information.* Prentice-Hall, New York, 1988.

[162] DHAR, S.B. : "Power System Long-Range Decision Analysis Under Fuzzy Environment", in *IEEE Transactions on Power Apparatus and Systems*, vol. 98, no. 2, pp. 585–596, 1979.

[163] ECONOMAKOS, E. : "Application of Fuzzy Concepts to Power Demand Forecasting", in *IEEE Transactions on Systems, Man and Cybernetics*, vol. 9, no. 10, pp. 651–657, 1979.

[164] KUO, H.C. AND HSU, Y.Y. : "Distribution System Load Estimation and Service Restoration Using a Fuzzy Set Approach", in *IEEE Transactions on Power Delivery*, vol. 8, no. 4, pp. 1950–1957, 1993.

[165] SOUFLIS, J.L., MACHIAS, A.V., AND PAPADIAS, B.C. : "An Application of Fuzzy Concepts to Transient Stability Evaluation", in *IEEE Transactions on Power Systems*, vol. 4, no. 3, pp. 1003–1009, 1989.

[166] RAFIAN, M., STERLING, M.J.H., AND IRVING, M.R. : "Real-Time Power System Simulation", in *Proceedings of the IEE, Part C - Generation, Transmission and Distribution*, vol. 134, no. 3, pp. 206–223, 1987.

[167] RAFIAN, M., STERLING, M.J.H., AND IRVING, M.R. : "Parallel Processing Algorithm for Power System Simulation", in *Proceedings of the IEE, Part C - Generation, Transmission and Distribution*, vol. 135, no. 4, pp. 285–290, 1988.

[168] DALE, L.A. : *Real-Time Modelling of Multi-Machine Power Systems.* PhD thesis, University of Bath, School of Electronic & Electrical Engineering, 1986.

[169] BERRY, T. : *Real-Time Simulation of Complex Power Systems Using Parallel Processors.* PhD thesis, University of Bath, School of Electronic & Electrical Engineering, 1989.

[170] CHAN, K.W. : *A Real-Time Simulation of the British National Supergrid.* PhD thesis, University of Bath, School of Electronic & Electrical Engineering, 1992.

[171] STAGG, T.A. : *A Parallel Computer Based Study of the Automatic Control of Power Generation.* PhD thesis, University of Bath, School of Electronic & Electrical Engineering, 1992.

[172] IEEE COMMITTEE REPORT, "Computer Representations of Excitation Systems", in *IEEE Transactions on Power Apparatus and Systems*, vol. 100, no. 2, pp. 494–509, 1981.

[173] IEEE COMMITTEE REPORT, "Dynamic Models for Steam and Hydro Turbines in Power System Studies", in *IEEE Transactions on Power Apparatus and Systems*, vol. 92, no. 1, pp. 1904–1915, 1973.

[174] DONOVAN, A.J. AND FLOOD, S.A. : "OPFL02 : A Note on a New Version of the Computer Power Flow Program OPFL0", Tech. Rep., CISD/CC/N916, CEGB Computing Centre, 1985.

[175] NG, F. : *A Man-Machine Interface for Real Time Power System Simulation.* PhD thesis, University of Bath, School of Electronic & Electrical Engineering, 1992.

[176] MICROWAY INC., USA, "Number Smasher-860 Owner's Manual", Tech. Rep., Microway Inc. and Research Park, Box 79, Kingston, USA, 1990.

[177] MICROWAY (EUROPE) LIMITED, "Product Information", Tech. Rep., Microway (Europe) Limited, 32 High Street, Kingston-Upon-Thames, Surrey, KT1 1HL, UK, 1992.

[178] MICROWAY (EUROPE) LIMITED, "NDP Software Manual (Version 4.1d for DOS)", Tech. Rep., Microway (Europe) Limited, 32 High Street, Kingston-Upon-Thames, Surrey, KT1 1HL, UK, 1992.

[179] SILICON GRAPHICS, COMPUTING SYSTEMS, "Indigo Product Guide", Tech. Rep., Silicon Graphics, Computing Systems, 1530 Arlington Business Park, Theale, Reading, Berks RG7 4SB, 1993.

[180] BACH, M.J. : *The Design of the UNIX Operating System.* Prentice-Hall, 1991.

[181] O'REILLY, T. : *X Windows System User's Guide.* O'Reilly and Associates, 1988.

[182] DANIELS, A.R., DUNN, R.W., PADGET, J.A., AND CHAN, K.W. : "On-Line Dynamic Security Assessor, Technical Update Report for SERC", Tech. Rep., University of Bath, School of Electronic & Electrical Engineering, 1993.

[183] SCHILDT, H. : *C: The Complete Reference.* McGraw-Hill, 1987.

[184] HARBISON, S.P. AND STEELE JR., G.L. : *C: A Reference Manual.* Prentice-Hall, 2^{nd} ed., 1987.

[185] KERNIGHAN, B.W. AND RITCHIE, D.M. : *The C Programming Language.* Prentice-Hall, 2^{nd} ed., 1988.

[186] GILCHRIST, F.J. AND MARR, E.J. : "RACE01 - A.C. Reduction Program", Tech. Rep., CC/P510, CEGB Computing Services Department.

[187] FRERIS, L.L. AND SASSON, A.M. : "Investigation of the load flow problem", in *Proceedings of the IEEE*, vol. 115, pp. 1459–1470, 1968.

[188] SPRATELEY, R.B. : "The Transient Stability Program RASM06", Tech. Rep., CISD/CC/N992, CEGB Computing Centre, 1987.

[189] GEC MEASUREMENTS LIMITED, *Protective Relays Application Guide.* GEC Alsthom Measurements Limited, St Leonards Works, Stafford, UK, 3^{rd} ed., 1987.

[190] CHAN, K.W. : "Progress Report for NGC/SERC DSA Research Grant", Tech. Rep., University of Bath, School of Electronic & Electrical Engineering, 1994.

Appendix A

20 Machine and 100 Busbar Results

A.1 Contingency Database

```
*
*          Example Contingency List for m20b100 study
*
*     4    double transmission line circuit outages
*     4    single transmission line circuit outages
*     6    3-phase busbar faults
*     6    network load losses
*     6    generator group trips
*   ----
*    26    contingencies in total
*


contg start


* Double Line Outages

contg line STEW2J-ECCL2Q:L1 side local
contg and line COCK2-STEW2J:L1 side local

contg line DEES4-PENT4:L2 side remote
contg and line DEES4-PENT4:L1 side remote

contg line NORT4R-OSBA4Q:L1 side remote
contg and line NORT4R-HAWP2:L1 side remote

contg line KIBY2-HEYS4:L1 side remote
contg and line FIDF2J-HEYS4:L1 side remote
```

```
* Single Line Outages

contg line CRUA2Q-WIYH2:L1 side local
contg line BRLE4-WWEY2K:L1 side local
contg line INDQ4-TAUN4Q:L1 side remote
contg line EGGB4J-PEWO4:L1 side remote


* Busbar Faults

contg bbar EGGB4J
contg bbar WBUR4
contg bbar DRAK4
contg bbar SUND4
contg bbar MELK4
contg bbar KINC2


* Load Losses

contg load DRAX4J
contg load FIDF2J
contg load HUER4
contg load PELH4
contg load WALH4
contg load IRON4


* Group Trips

contg group WYLFA
contg group HINKLEY
contg group DRAX.B
contg group DUNGENESS
contg group LONGANNET
contg group RATCLIFFE


contg end screen 1.0 duration 80.0 analysis 10.0 stability 60.0
```

A.2 Results Summary

Results Obtained During Contingency Analysis	System Operating Condition	
	Base Case (Scotland-England Transfer = 500 MW)	Stressed Case (Scotland-England Transfer = 920 MW)
Total no. of Entries in Contingency Database	26	26
Total no. of Ranked Contingencies after Analysis	22	26
Total no. of Transiently Unstable Contingencies	2	13
Total no. of Dynamically Unstable Contingencies	0	6

Table A.1: Results summary for two 20 machine and 100 busbar model scenarios

A.3 Ranking Summary

Contingency Name	System Operating Condition			
	Base Case		Stressed Case	
	Ranking	Stability	Ranking	Stability
Line STEW2J-ECCL2Q:L1 Line COCK2-STEW2J:L1	15	Stable	3	Transient
Line DEES4-PENT4:L2 Line DEES4-PENT4:L1	1	Transient	9	Transient
Line NORT4R-OSBA4Q:L1 Line NORT4R-HAWP2:L1	3	Stable	11	Transient
Line KIBY2-HEYS4:L1 Line FIDF2J-HEYS4:L1	9	Stable	17	Dynamic
Line CRUA2Q-WIYH2:L1	2	Transient	13	Transient
Line BRLE4-WWEY2K:L1	10	Stable	7	Transient
Line INDQ4-TAUN4Q:L1	16	Stable	19	Dynamic
Line EGGB4J-PEWO4:L1	6	Stable	18	Dynamic
Busbar EGGB4J	4	Stable	8	Transient
Busbar WBUR4	5	Stable	4	Transient
Busbar DRAK4	8	Stable	10	Transient
Busbar SUND4	11	Stable	2	Transient
Busbar MELK4	12	Stable	6	Transient
Busbar KINC2	13	Stable	12	Transient

continued on next page

continued from previous page

Contingency Name	System Operating Condition			
	Base Case		Stressed Case	
	Ranking	Stability	Ranking	Stability
Load Busbar DRAX4J	18	Stable	23	Stable
Load Busbar FIDF2J	21	Stable	24	Stable
Load Busbar HUER4	-	-	16	Dynamic
Load Busbar PELH4	-	-	25	Stable
Load Busbar WALH4	-	-	20	Stable
Load Busbar IRON4	-	-	22	Stable
Group WYLFA	20	Stable	14	Dynamic
Group HINKLEY	14	Stable	15	Dynamic
Group DRAX.B	7	Stable	1	Transient
Group DUNGENESS	17	Stable	21	Stable
Group LONGANNET	22	Stable	26	Stable
Group RATCLIFFE	19	Stable	5	Transient

Table A.3: Summary of Contingency Rankings and Stabilities for two 20 machine and 100 busbar model scenarios

Appendix B

20 Machine and 100 Busbar Outputs (Base Case Condition)

B.1 General Alarm Summary Format

```
Fuzzy Logic Contingency Ranking and Alarm Processing Summary File

Sumrank :-  Screening Interval              1.00   secs
            Fault Duration                  0.08   secs
            Short Term Dynamics            10.00   secs
            Longer Term Dynamics           60.00   secs

            No. of Line Contingencies          8
            No. of Busbar Contingencies        6
            No. of Load Contingencies          6
            No. of Group Contingencies         6

            Total No. of Contingencies        26

Contingency Listing System Security Assessment Cycle completed in 6:54 mins

Contingency             Limit Violations/Alarms          System Stability

Line DEES4-PENT4:L1     1 Group pole-slipped             Transient Instability
Line DEES4-PENT4:L2     7 Line Overload Violations
(Remote End Tripped)    100 Voltage Violations
                        1 System Frequency Violation
                        8 Group MW Limit Violations
                        3 Group MVAr Limit Violations

Line CRUA2Q-WIYH2:L1    1 Group pole-slipped             Transient Instability
(Local End Tripped)     1 Busbar islanded
                        2 Line Overload Violations
                        35 Voltage Violations
                        1 Group MW Limit Violation

Line NORT4R-HAWP2:L1    1 Busbar islanded
Line NORT4R-OSBA4Q:L1   3 Line Overload Violations
(Remote End Tripped)    99 Voltage Violations
                        8 Group MW Limit Violations
```

Contingency	Limit Violations/Alarms	System Stability
	1 Group MVAr Limit Violation	
Busbar EGGB4J	6 Line Overload Violations 100 Voltage Violations 8 Group MW Limit Violations	
Busbar WBUR4	4 Line Overload Violations 100 Voltage Violations 10 Group MW Limit Violations	
Line EGGB4J-PEWO4:L1 (Remote End Tripped)	7 Line Overload Violations 100 Voltage Violations 10 Group MW Limit Violations	
Group DRAX.B	2 Line Overload Violations 100 Voltage Violations 12 Group MW Limit Violations 9 Group MVAr Limit Violations	
Busbar DRAK4	5 Line Overload Violations 100 Voltage Violations 6 Group MW Limit Violations 2 Group MVAr Limit Violations	
Line FIDF2J-HEYS4:L1 Line KIBY2-HEYS4:L1 (Remote End Tripped)	6 Line Overload Violations 100 Voltage Violations 7 Group MW Limit Violations	
Line BRLE4-WWEY2K:L1 (Local End Tripped)	4 Line Overload Violations 95 Voltage Violations 4 Group MW Limit Violations 1 Group MVAr Limit Violation	
Busbar SUND4	2 Line Overload Violations 96 Voltage Violations 4 Group MW Limit Violations 2 Group MVAr Limit Violations	
Busbar MELK4	2 Line Overload Violations 90 Voltage Violations 3 Group MW Limit Violations 1 Group MVAr Limit Violation	
Busbar KINC2	2 Line Overload Violations 78 Voltage Violations 3 Group MW Limit Violations 1 Group MVAr Limit Violation	
Group HINKLEY	1 Line Overload Violation 14 Voltage Violations 3 Group MW Limit Violations 1 Group MVAr Limit Violation	

Contingency	Limit Violations/Alarms	System Stability
Line COCK2-STEW2J:L1	3 Line Overload Violations	
Line STEW2J-ECCL2Q:L1	40 Voltage Violations	
(Local End Tripped)	3 Group MW Limit Violations	
	2 Group MVAr Limit Violations	
Line INDQ4-TAUN4Q:L1	1 Line Overload Violation	
(Remote End Tripped)	43 Voltage Violations	
	2 Group MW Limit Violations	
Group DUNGENESS	1 Line Overload Violation	
	3 Voltage Violations	
	4 Group MW Limit Violations	
	1 Group MVAr Limit Violation	
Load DRAX4J	1 Line Overload Violation	
Group RATCLIFFE	1 Line Overload Violation	
	1 Voltage Violation	
	1 Group MW Limit Violation	
Group WYLFA	1 Line Overload Violation	
Load FIDF2J	1 Line Overload Violation	
Group LONGANNET	1 Line Overload Violation	
	1 System Frequency Violation	
	2 Group MW Limit Violations	
	3 Group MVAr Limit Violations	

B.2 Geographical Specific Alarm Summary Format

```
        Fuzzy Logic Contingency Ranking and Alarm Processing Summary File

    Sumrank :-  Screening Interval            1.00   secs
                Fault Duration                0.08   secs
                Short Term Dynamics          10.00   secs
                Longer Term Dynamics         60.00   secs

                No. of Line Contingencies        8
                No. of Busbar Contingencies      6
                No. of Load Contingencies        6
                No. of Group Contingencies       6

                Total No. of Contingencies      26


     Contingency Listing System Security Assessment Cycle completed in 6:54 mins

Contingency           Limit Violations/Alarms                  System Stability

Line DEES4-PENT4:L1   1 Group pole-slipped (Leeds)             Transient Instability
Line DEES4-PENT4:L2   7 Line Overload Violations (Leeds)
(Remote End Tripped)  17 Voltage Violations (Scotland)
                      33 Voltage Violations (Leeds)
                      12 Voltage Violations (Birmingham)
                      21 Voltage Violations (St Albans)
                      17 Voltage Violations (Bristol)
                      1 System Frequency Violation
                      1 Group MW Limit Violation (Scotland)
                      5 Group MW Limit Violations (Leeds)
                      2 Group MW Limit Violations (Birmingham)
                      3 Group MVAr Limit Violations (Leeds)

Line CRUA2Q-WIYH2:L1  1 Group pole-slipped (Scotland)          Transient Instability
(Local End Tripped)   1 Busbar islanded (Scotland)
                      2 Line Overload Violations (Leeds)
                      16 Voltage Violations (Scotland)
                      12 Voltage Violations (Leeds)
                      7 Voltage Violations (St Albans)
                      1 Group MW Limit Violation (Leeds)

Line NORT4R-HAWP2:L1  1 Busbar islanded (Leeds)
Line NORT4R-OSBA4Q:L1 3 Line Overload Violations (Leeds)
(Remote End Tripped)  17 Voltage Violations (Scotland)
                      32 Voltage Violations (Leeds)
                      12 Voltage Violations (Birmingham)
                      21 Voltage Violations (St Albans)
                      17 Voltage Violations (Bristol)
                      1 Group MW Limit Violation (Scotland)
                      5 Group MW Limit Violations (Leeds)
                      2 Group MW Limit Violations (Birmingham)
                      1 Group MVAr Limit Violation (Leeds)
```

Contingency	Limit Violations/Alarms	System Stability
Busbar EGGB4J	1 Line Overload Violation (Scotland) 4 Line Overload Violations (Leeds) 1 Line Overload Violation (Birmingham) 17 Voltage Violations (Scotland) 33 Voltage Violations (Leeds) 12 Voltage Violations (Birmingham) 21 Voltage Violations (St Albans) 17 Voltage Violations (Bristol) 2 Group MW Limit Violations (Scotland) 4 Group MW Limit Violations (Leeds) 2 Group MW Limit Violations (Birmingham)	
Busbar WBUR4	1 Line Overload Violation (Scotland) 3 Line Overload Violations (Leeds) 17 Voltage Violations (Scotland) 33 Voltage Violations (Leeds) 12 Voltage Violations (Birmingham) 21 Voltage Violations (St Albans) 17 Voltage Violations (Bristol) 2 Group MW Limit Violations (Scotland) 5 Group MW Limit Violations (Leeds) 3 Group MW Limit Violations (Birmingham)	
Line EGGB4J-PEW04:L1 (Remote End Tripped)	6 Line Overload Violations (Leeds) 1 Line Overload Violation (Birmingham) 17 Voltage Violations (Scotland) 33 Voltage Violations (Leeds) 12 Voltage Violations (Birmingham) 21 Voltage Violations (St Albans) 17 Voltage Violations (Bristol) 2 Group MW Limit Violations (Scotland) 7 Group MW Limit Violations (Leeds) 1 Group MW Limit Violation (Birmingham)	
Group DRAX.B	1 Line Overload Violation (Scotland) 1 Line Overload Violation (Leeds) 17 Voltage Violations (Scotland) 33 Voltage Violations (Leeds) 12 Voltage Violations (Birmingham) 21 Voltage Violations (St Albans) 17 Voltage Violations (Bristol) 1 Group MW Limit Violation (Scotland) 8 Group MW Limit Violations (Leeds) 3 Group MW Limit Violations (Birmingham) 6 Group MVAr Limit Violations (Leeds) 3 Group MVAr Limit Violations (Birmingham)	
Busbar DRAK4	4 Line Overload Violations (Leeds) 1 Line Overload Violation (Birmingham) 17 Voltage Violations (Scotland) 33 Voltage Violations (Leeds) 12 Voltage Violations (Birmingham) 21 Voltage Violations (St Albans) 17 Voltage Violations (Bristol) 1 Group MW Limit Violation (Scotland)	

Contingency	Limit Violations/Alarms	System Stability
	5 Group MW Limit Violations (Leeds)	
	1 Group MVAr Limit Violation (Leeds)	
	1 Group MVAr Limit Violation (Birmingham)	
Line FIDF2J-HEYS4:L1	6 Line Overload Violations (Leeds)	
Line KIBY2-HEYS4:L1	17 Voltage Violations (Scotland)	
(Remote End Tripped)	33 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	
	1 Group MW Limit Violation (Scotland)	
	6 Group MW Limit Violations (Leeds)	
Line BRLE4-WWEY2K:L1	2 Line Overload Violations (Leeds)	
(Local End Tripped)	2 Line Overload Violations (St Albans)	
	13 Voltage Violations (Scotland)	
	33 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	16 Voltage Violations (Bristol)	
	1 Group MW Limit Violation (Scotland)	
	3 Group MW Limit Violations (Leeds)	
	1 Group MVAr Limit Violation (Leeds)	
Busbar SUND4	2 Line Overload Violations (Leeds)	
	14 Voltage Violations (Scotland)	
	33 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	16 Voltage Violations (Bristol)	
	1 Group MW Limit Violation (Scotland)	
	3 Group MW Limit Violations (Leeds)	
	1 Group MVAr Limit Violation (Leeds)	
	1 Group MVAr Limit Violation (Birmingham)	
Busbar MELK4	2 Line Overload Violations (Leeds)	
	12 Voltage Violations (Scotland)	
	33 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	12 Voltage Violations (Bristol)	
	1 Group MW Limit Violation (Scotland)	
	2 Group MW Limit Violations (Leeds)	
	1 Group MVAr Limit Violation (Leeds)	
Busbar KINC2	2 Line Overload Violations (Leeds)	
	17 Voltage Violations (Scotland)	
	32 Voltage Violations (Leeds)	
	11 Voltage Violations (Birmingham)	
	15 Voltage Violations (St Albans)	
	3 Voltage Violations (Bristol)	
	2 Group MW Limit Violations (Scotland)	
	1 Group MW Limit Violation (Leeds)	
	1 Group MVAr Limit Violation (Scotland)	

Contingency	Limit Violations/Alarms	System Stability
Group HINKLEY	1 Line Overload Violation (Leeds) 2 Voltage Violations (St Albans) 12 Voltage Violations (Bristol) 3 Group MW Limit Violations (Birmingham) 1 Group MVAr Limit Violation (St Albans)	
Line COCK2-STEW2J:L1 Line STEW2J-ECCL2Q:L1 (Local End Tripped)	1 Line Overload Violation (Scotland) 2 Line Overload Violations (Leeds) 17 Voltage Violations (Scotland) 14 Voltage Violations (Leeds) 9 Voltage Violations (St Albans) 2 Group MW Limit Violations (Scotland) 1 Group MW Limit Violation (Leeds) 2 Group MVAr Limit Violations (Scotland)	
Line INDQ4-TAUM4Q:L1 (Remote End Tripped)	1 Line Overload Violation (Leeds) 5 Voltage Violations (Scotland) 23 Voltage Violations (Leeds) 1 Voltage Violation (Birmingham) 11 Voltage Violations (St Albans) 3 Voltage Violations (Bristol) 1 Group MW Limit Violation (Scotland) 1 Group MW Limit Violation (Leeds)	
Group DUNGENESS	1 Line Overload Violation (Leeds) 3 Voltage Violations (Bristol) 1 Group MW Limit Violation (Leeds) 3 Group MW Limit Violations (Birmingham) 1 Group MVAr Limit Violation (Bristol)	
Load DRAX4J	1 Line Overload Violation (Leeds)	
Group RATCLIFFE	1 Line Overload Violation (Leeds) 1 Voltage Violation (Bristol) 1 Group MW Limit Violation (Birmingham)	
Group WYLFA	1 Line Overload Violation (Leeds)	
Load FIDF2J	1 Line Overload Violation (Leeds)	
Group LONGANNET	1 Line Overload Violation (Leeds) 1 System Frequency Violation 2 Group MW Limit Violations (Scotland) 3 Group MVAr Limit Violations (Scotland)	

B.3 Full Alarm List Format

B.3.1 Top Transiently Unstable Contingency

Fuzzy Logic Contingency Ranking and Alarm Processing Summary File

Sumrank :-	Screening Interval	1.00	secs
	Fault Duration	0.08	secs
	Short Term Dynamics	10.00	secs
	Longer Term Dynamics	60.00	secs
	No. of Line Contingencies	8	
	No. of Busbar Contingencies	6	
	No. of Load Contingencies	6	
	No. of Group Contingencies	6	
	Total No. of Contingencies	26	

Contingency Listing System Security Assessment Cycle completed in 6:54 mins

Contingency	Limit Violations/Alarms	System Stability
Line DEES4-PENT4:L1	Frequency 50.42 Hz	Transient Instability
Line DEES4-PENT4:L2	Line DEES4-FIDF2J:L1 - Overload 87.1%	
(Remote End Tripped)	Line DEES4-TRAW4:L1 - Overload 107.6%	
	Line DINO4-PENT4:L2 - Overload 88.9%	
	Line DRAX4J-KEAD4:L1 - Overload 88.2%	
	Line LEGA4-TRAW4:L1 - Overload 85.6%	
	Line PENT4-TRAW4:L1 - Overload 164.9%	
	Busbar ABTH2J - Voltage 0.94 pu	
	Busbar BLYT2J - Voltage 0.82 pu	
	Busbar BRFO4 - Voltage 0.77 pu	
	Busbar BRLE4 - Voltage 0.74 pu	
	Busbar CANT4 - Voltage 0.80 pu	
	Busbar CAPE2J - Voltage 0.40 pu	
	Busbar CELL4 - Voltage 0.60 pu	
	Busbar CILF4 - Voltage 0.69 pu	
	Busbar CLYM2 - Voltage 0.91 pu	
	Busbar COCK2 - Voltage 0.89 pu	
	Busbar COTT4 - Voltage 1.08 pu	
	Busbar COWL4 - Voltage 1.07 pu	
	Busbar CREB4 - Voltage 0.78 pu	
	Busbar CRUA2Q - Voltage 0.94 pu	
	Busbar DAIN4 - Voltage 0.51 pu	
	Busbar DEES4 - Voltage 0.86 pu	
	Busbar DIDC4 - Voltage 1.07 pu	
	Busbar DINO4 - Voltage 0.54 pu	
	Busbar DRAK4 - Voltage 0.62 pu	
	Busbar DRAX4J - Voltage 0.79 pu	
	Busbar DUNG4 - Voltage 1.05 pu	
	Busbar ECCL2Q - Voltage 0.87 pu	
	Busbar ECLA4 - Voltage 0.73 pu	
	Busbar EGGB4J - Voltage 0.77 pu	

Contingency	Limit Violations/Alarms	System Stability
	Busbar ELST2J - Voltage 1.05 pu	
	Busbar EXET4 - Voltage 1.07 pu	
	Busbar FECK4 - Voltage 0.62 pu	
	Busbar FERR2J - Voltage 0.79 pu	
	Busbar FFES2 - Voltage 0.28 pu	
	Busbar FIDF2J - Voltage 0.49 pu	
	Busbar FOYE2 - Voltage 1.05 pu	
	Busbar GALA1 - Voltage 1.05 pu	
	Busbar GRAI4 - Voltage 0.79 pu	
	Busbar HAMH4 - Voltage 0.62 pu	
	Busbar HARK2 - Voltage 1.05 pu	
	Busbar HATL2 - Voltage 0.83 pu	
	Busbar HAWP2 - Voltage 0.82 pu	
	Busbar HEYS4 - Voltage 1.10 pu	
	Busbar HIGM4 - Voltage 1.08 pu	
	Busbar HINP4 - Voltage 1.08 pu	
	Busbar HUER4 - Voltage 0.94 pu	
	Busbar INDQ4 - Voltage 0.75 pu	
	Busbar IROW4 - Voltage 0.51 pu	
	Busbar IVER2J - Voltage 1.05 pu	
	Busbar KEAD4 - Voltage 0.77 pu	
	Busbar KEAR4Q - Voltage 1.08 pu	
	Busbar KEMS4J - Voltage 0.79 pu	
	Busbar KIBY2 - Voltage 0.51 pu	
	Busbar KILS2 - Voltage 0.91 pu	
	Busbar KINC2 - Voltage 0.92 pu	
	Busbar KINO4 - Voltage 0.79 pu	
	Busbar KINT2 - Voltage 1.05 pu	
	Busbar LEGA4 - Voltage 0.38 pu	
	Busbar LITT4 - Voltage 0.78 pu	
	Busbar LOAN2 - Voltage 0.93 pu	
	Busbar LOVE4 - Voltage 1.05 pu	
	Busbar MAYT1T - Voltage 0.88 pu	
	Busbar MELK4 - Voltage 1.06 pu	
	Busbar NEIL2 - Voltage 0.92 pu	
	Busbar NFLW4R - Voltage 0.79 pu	
	Busbar NFLW4S - Voltage 0.78 pu	
	Busbar NORT2 - Voltage 0.82 pu	
	Busbar NORT4R - Voltage 0.81 pu	
	Busbar OSBA4Q - Voltage 0.79 pu	
	Busbar PEHE2 - Voltage 1.05 pu	
	Busbar PELH4 - Voltage 1.08 pu	
	Busbar PEMB4 - Voltage 0.69 pu	
	Busbar PENN2 - Voltage 0.56 pu	
	Busbar PENT4 - Voltage 0.53 pu	
	Busbar PEWO4 - Voltage 1.06 pu	
	Busbar RATS4J - Voltage 1.07 pu	
	Busbar RUGE4 - Voltage 0.61 pu	
	Busbar STAL4Q - Voltage 1.08 pu	
	Busbar STEW2J - Voltage 0.83 pu	
	Busbar STHA2 - Voltage 0.90 pu	
	Busbar STSB4 - Voltage 1.09 pu	
	Busbar SUND4 - Voltage 1.05 pu	
	Busbar SWAN4 - Voltage 0.69 pu	
	Busbar TAUN4Q - Voltage 1.08 pu	

Contingency	Limit Violations/Alarms	System Stability
	Busbar TAUM4R - Voltage 1.08 pu	
	Busbar THOM2J - Voltage 1.09 pu	
	Busbar THOM4 - Voltage 1.08 pu	
	Busbar TILB4R - Voltage 0.79 pu	
	Busbar TRAW2 - Voltage 0.28 pu	
	Busbar TRAW4 - Voltage 0.21 pu	
	Busbar WALH4 - Voltage 0.68 pu	
	Busbar WALP4 - Voltage 1.08 pu	
	Busbar WALX4Q - Voltage 1.08 pu	
	Busbar WALX4R - Voltage 1.08 pu	
	Busbar WBOL2 - Voltage 0.82 pu	
	Busbar WBUR4 - Voltage 1.08 pu	
	Busbar WHSO2 - Voltage 0.94 pu	
	Busbar WHSO4Q - Voltage 0.70 pu	
	Busbar WILL4 - Voltage 1.07 pu	
	Busbar WISD2 - Voltage 0.77 pu	
	Busbar WISH2 - Voltage 0.90 pu	
	Busbar WIYH2 - Voltage 1.05 pu	
	Busbar WTHU2J - Voltage 1.08 pu	
	Busbar WWEY2K - Voltage 1.05 pu	
	Busbar WYLF4 - Voltage 0.53 pu	
	Group CRUACHAN - on MW Limits	
	Group DINORWIG - on MW Limits	
	Group DINORWIG - on MVAr Limits	
	Group FFESTIN. - on MVAr Limits	
	Group FIDDLERS - on MW Limits	
	Group RATCLIFFE - on MW Limits	
	Group RUGELEY - on MW Limits	
	Group DINORWIG (pole-slipped)	
	Line DINO4-PENT4:L1 - Overload 126.7%	
	Group FFESTIN. - on MW Limits	
	Group TRAWS. - on MW Limits	
	Group TRAWS. - on MVAr Limits	
	Group WYLFA - on MW Limits	

B.3.2 Top Stable Contingency

Fuzzy Logic Contingency Ranking and Alarm Processing Summary File

Sumrank :-	Screening Interval	1.00	secs
	Fault Duration	0.08	secs
	Short Term Dynamics	10.00	secs
	Longer Term Dynamics	60.00	secs
	No. of Line Contingencies	8	
	No. of Busbar Contingencies	6	
	No. of Load Contingencies	6	
	No. of Group Contingencies	6	
	Total No. of Contingencies	26	

Contingency Listing System Security Assessment Cycle completed in 6:54 mins

Contingency	Limit Violations/Alarms	System Stability
Line NORT4R-HAWP2:L1	Busbar NORT4R islanded	
Line NORT4R-OSBA4Q:L1	Line DINO4-PENT4:L2 - Overload 85.9%	
(Remote End Tripped)	Line DRAX4J-KEAD4:L1 - Overload 86.9%	
	Line HARK2-STHA2:L1 - Overload 85.2%	
	Busbar ABTH2J - Voltage 1.06 pu	
	Busbar BLYT2J - Voltage 1.05 pu	
	Busbar BRFO4 - Voltage 1.06 pu	
	Busbar BRLE4 - Voltage 0.71 pu	
	Busbar CANT4 - Voltage 1.06 pu	
	Busbar CAPE2J - Voltage 1.07 pu	
	Busbar CELL4 - Voltage 1.06 pu	
	Busbar CILF4 - Voltage 0.70 pu	
	Busbar CLYN2 - Voltage 0.74 pu	
	Busbar COCK2 - Voltage 1.06 pu	
	Busbar COTT4 - Voltage 0.55 pu	
	Busbar COWL4 - Voltage 1.06 pu	
	Busbar CREB4 - Voltage 0.46 pu	
	Busbar CRUA2Q - Voltage 1.05 pu	
	Busbar DAIN4 - Voltage 1.06 pu	
	Busbar DEES4 - Voltage 0.71 pu	
	Busbar DIDC4 - Voltage 1.06 pu	
	Busbar DINO4 - Voltage 1.06 pu	
	Busbar DRAK4 - Voltage 1.06 pu	
	Busbar DRAX4J - Voltage 0.44 pu	
	Busbar DUNG4 - Voltage 0.77 pu	
	Busbar ECCL2Q - Voltage 0.48 pu	
	Busbar ECLA4 - Voltage 1.06 pu	
	Busbar EGGB4J - Voltage 0.47 pu	
	Busbar ELST2J - Voltage 0.67 pu	
	Busbar EXET4 - Voltage 1.06 pu	
	Busbar FECK4 - Voltage 1.06 pu	
	Busbar FERR2J - Voltage 0.44 pu	
	Busbar FFES2 - Voltage 0.78 pu	
	Busbar FIDF2J - Voltage 1.07 pu	

Contingency	Limit Violations/Alarms	System Stability
	Busbar FOYE2 - Voltage 0.88 pu	
	Busbar GALA1 - Voltage 1.06 pu	
	Busbar GRAI4 - Voltage 0.72 pu	
	Busbar HAMH4 - Voltage 1.06 pu	
	Busbar HARK2 - Voltage 1.06 pu	
	Busbar HATL2 - Voltage 0.13 pu	
	Busbar HAWP2 - Voltage 0.86 pu	
	Busbar HEYS4 - Voltage 1.06 pu	
	Busbar HIGM4 - Voltage 0.56 pu	
	Busbar HINP4 - Voltage 1.06 pu	
	Busbar HUER4 - Voltage 1.06 pu	
	Busbar INDQ4 - Voltage 0.75 pu	
	Busbar IRON4 - Voltage 1.06 pu	
	Busbar IVER2J - Voltage 1.06 pu	
	Busbar KEAD4 - Voltage 0.50 pu	
	Busbar KEAR4Q - Voltage 0.51 pu	
	Busbar KEMS4J - Voltage 0.72 pu	
	Busbar KIBY2 - Voltage 0.68 pu	
	Busbar KILS2 - Voltage 1.05 pu	
	Busbar KINC2 - Voltage 0.73 pu	
	Busbar KINO4 - Voltage 1.07 pu	
	Busbar KINT2 - Voltage 1.05 pu	
	Busbar LEGA4 - Voltage 0.71 pu	
	Busbar LITT4 - Voltage 1.06 pu	
	Busbar LOAN2 - Voltage 1.06 pu	
	Busbar LOVE4 - Voltage 0.73 pu	
	Busbar MAYT1T - Voltage 1.05 pu	
	Busbar MELK4 - Voltage 1.05 pu	
	Busbar MEIL2 - Voltage 0.77 pu	
	Busbar MFLW4R - Voltage 1.05 pu	
	Busbar MFLW4S - Voltage 1.06 pu	
	Busbar MORT2 - Voltage 0.14 pu	
	Busbar OSBA4Q - Voltage 0.84 pu	
	Busbar PEHE2 - Voltage 1.05 pu	
	Busbar PELH4 - Voltage 0.65 pu	
	Busbar PEMB4 - Voltage 1.05 pu	
	Busbar PENN2 - Voltage 0.69 pu	
	Busbar PENT4 - Voltage 1.06 pu	
	Busbar PEWO4 - Voltage 0.60 pu	
	Busbar RATS4J - Voltage 1.06 pu	
	Busbar RUGE4 - Voltage 1.06 pu	
	Busbar STAL4Q - Voltage 1.06 pu	
	Busbar STEW2J - Voltage 1.06 pu	
	Busbar STHA2 - Voltage 0.73 pu	
	Busbar STSB4 - Voltage 1.05 pu	
	Busbar SUND4 - Voltage 1.06 pu	
	Busbar SWAN4 - Voltage 0.70 pu	
	Busbar TAUN4Q - Voltage 1.06 pu	
	Busbar TAUN4R - Voltage 1.06 pu	
	Busbar THOM2J - Voltage 0.50 pu	
	Busbar THOM4 - Voltage 1.06 pu	
	Busbar TILB4R - Voltage 0.71 pu	
	Busbar TRAW2 - Voltage 0.77 pu	
	Busbar TRAW4 - Voltage 0.75 pu	
	Busbar WALH4 - Voltage 1.06 pu	

Contingency	Limit Violations/Alarms	System Stability
	Busbar WALP4 - Voltage 0.62 pu	
	Busbar WALX4Q - Voltage 0.66 pu	
	Busbar WALX4R - Voltage 0.66 pu	
	Busbar WBOL2 - Voltage 0.12 pu	
	Busbar WBUR4 - Voltage 0.55 pu	
	Busbar WHSO2 - Voltage 0.70 pu	
	Busbar WHSO4Q - Voltage 0.71 pu	
	Busbar WILL4 - Voltage 1.06 pu	
	Busbar WISD2 - Voltage 1.06 pu	
	Busbar WISH2 - Voltage 1.05 pu	
	Busbar WIYH2 - Voltage 1.05 pu	
	Busbar WTHU2J - Voltage 1.05 pu	
	Busbar WWEY2K - Voltage 0.69 pu	
	Busbar WYLF4 - Voltage 1.05 pu	
	Group CRUACHAN - on MW Limits	
	Group DINORWIG - on MW Limits	
	Group DINORWIG - on MVAr Limits	
	Group FERRYBR. - on MW Limits	
	Group HARTLEPL. - on MW Limits	
	Group RATCLIFFE - on MW Limits	
	Group RUGELEY - on MW Limits	
	Group TRAWS. - on MW Limits	
	Group WYLFA - on MW Limits	

Appendix C

20 Machine and 100 Busbar Outputs (Stressed Condition)

C.1 General Alarm Summary Format

Fuzzy Logic Contingency Ranking and Alarm Processing Summary File

Sumrank :-	Screening Interval	1.00	secs
	Fault Duration	0.08	secs
	Short Term Dynamics	10.00	secs
	Longer Term Dynamics	60.00	secs
	No. of Line Contingencies	8	
	No. of Busbar Contingencies	6	
	No. of Load Contingencies	6	
	No. of Group Contingencies	6	
	Total No. of Contingencies	26	

Contingency Listing System Security Assessment Cycle completed in 9:49 mins

Contingency	Limit Violations/Alarms	System Stability
Group DRAX.B	1 Group pole-slipped	Transient Instability
	28 Line Overload Violations	
	100 Voltage Violations	
	13 Group MW Limit Violations	
	8 Group MVAr Limit Violations	
Busbar SUND4	1 Group pole-slipped	Transient Instability
	18 Line Overload Violations	
	97 Voltage Violations	
	1 System Frequency Violation	
	15 Group MW Limit Violations	
	5 Group MVAr Limit Violations	
Line COCK2-STEW2J:L1	2 Groups pole-slipped	Transient Instability
Line STEW2J-ECCL2Q:L1	10 Line Overload Violations	
(Local End Tripped)	92 Voltage Violations	
	9 Group MW Limit Violations	

Contingency	Limit Violations/Alarms	System Stability
	2 Group MVAr Limit Violations	
Busbar WBUR4	1 Group pole-slipped 19 Line Overload Violations 100 Voltage Violations 1 System Frequency Violation 15 Group MW Limit Violations 10 Group MVAr Limit Violations	Transient Instability
Group RATCLIFFE	1 Group pole-slipped 23 Line Overload Violations 100 Voltage Violations 1 System Frequency Violation 12 Group MW Limit Violations 6 Group MVAr Limit Violations	Transient Instability
Busbar MELK4	1 Group pole-slipped 21 Line Overload Violations 99 Voltage Violations 1 System Frequency Violation 14 Group MW Limit Violations 5 Group MVAr Limit Violations	Transient Instability
Line BRLE4-WWEY2K:L1 (Local End Tripped)	1 Group pole-slipped 21 Line Overload Violations 100 Voltage Violations 1 System Frequency Violation 15 Group MW Limit Violations 6 Group MVAr Limit Violations	Transient Instability
Busbar EGGB4J	1 Group pole-slipped 21 Line Overload Violations 99 Voltage Violations 1 System Frequency Violation 16 Group MW Limit Violations 9 Group MVAr Limit Violations	Transient Instability
Line DEES4-PENT4:L1 Line DEES4-PENT4:L2 (Remote End Tripped)	1 Group pole-slipped 9 Line Overload Violations 89 Voltage Violations 1 System Frequency Violation 7 Group MW Limit Violations 5 Group MVAr Limit Violations	Transient Instability
Busbar DRAK4	1 Group pole-slipped 23 Line Overload Violations 93 Voltage Violations 1 System Frequency Violation 15 Group MW Limit Violations 7 Group MVAr Limit Violations	Transient Instability
Line NORT4R-HAWP2:L1 Line NORT4R-OSBA4Q:L1 (Remote End Tripped)	1 Group pole-slipped 1 Busbar islanded 16 Line Overload Violations 80 Voltage Violations	Transient Instability

Contingency	Limit Violations/Alarms	System Stability
	11 Group MW Limit Violations 9 Group MVAr Limit Violations	
Busbar KINC2	1 Group pole-slipped 20 Line Overload Violations 96 Voltage Violations 1 System Frequency Violation 11 Group MW Limit Violations 5 Group MVAr Limit Violations	Transient Instability
Line CRUA2Q-WIYH2:L1 (Local End Tripped)	1 Group pole-slipped 1 Busbar islanded 8 Line Overload Violations 81 Voltage Violations 4 Group MW Limit Violations	Transient Instability
Group WYLFA	15 Groups with undamped oscillations 8 Line Overload Violations 94 Voltage Violations 1 Group MW Limit Violation	Dynamic Instability
Group HINKLEY	12 Groups with undamped oscillations 8 Line Overload Violations 94 Voltage Violations 4 Group MW Limit Violations	Dynamic Instability
Load HUER4	7 Groups with undamped oscillations 8 Line Overload Violations 95 Voltage Violations	Dynamic Instability
Line FIDF2J-HEYS4:L1 Line KIBY2-HEYS4:L1 (Remote End Tripped)	6 Groups with undamped oscillations 12 Line Overload Violations 97 Voltage Violations 7 Group MW Limit Violations 2 Group MVAr Limit Violations	Dynamic Instability
Line EGGB4J-PEWO4:L1 (Remote End Tripped)	2 Groups with undamped oscillations 10 Line Overload Violations 94 Voltage Violations 9 Group MW Limit Violations 8 Group MVAr Limit Violations	Dynamic Instability
Line INDQ4-TAUN4Q:L1 (Remote End Tripped)	3 Groups with undamped oscillations 9 Line Overload Violations 96 Voltage Violations 4 Group MW Limit Violations	Dynamic Instability
Load WALH4	7 Line Overload Violations 71 Voltage Violations	
Group DUNGENESS	7 Line Overload Violations 94 Voltage Violations 5 Group MW Limit Violations	
Load IRON4	7 Line Overload Violations	

Contingency	Limit Violations/Alarms	System Stability
	66 Voltage Violations	
Load DRAX4J	7 Line Overload Violations 69 Voltage Violations	
Load FIDF2J	7 Line Overload Violations 86 Voltage Violations	
Load PELH4	6 Line Overload Violations 57 Voltage Violations	
Group LONGANNET	7 Line Overload Violations 71 Voltage Violations 1 System Frequency Violation 8 Group MW Limit Violations 3 Group MVAr Limit Violations	

C.2 Geographical Specific Alarm Summary Format

```
        Fuzzy Logic Contingency Ranking and Alarm Processing Summary File


            Sumrank :-   Screening Interval            1.00   secs
                         Fault Duration                0.08   secs
                         Short Term Dynamics          10.00   secs
                         Longer Term Dynamics         60.00   secs

                         No.  of Line Contingencies       8
                         No.  of Busbar Contingencies     6
                         No.  of Load Contingencies       6
                         No.  of Group Contingencies      6

                         Total No.  of Contingencies     26


      Contingency Listing System Security Assessment Cycle completed in 9:49 mins

Contingency    Limit Violations/Alarms                      System Stability

Group DRAX.B   1 Group pole-slipped (Scotland)              Transient Instability
               7 Line Overload Violations (Scotland)
               19 Line Overload Violations (Leeds)
               2 Line Overload Violations (Birmingham)
               17 Voltage Violations (Scotland)
               33 Voltage Violations (Leeds)
               12 Voltage Violations (Birmingham)
               21 Voltage Violations (St Albans)
               17 Voltage Violations (Bristol)
               8 Group MW Limit Violations (Leeds)
               3 Group MW Limit Violations (Birmingham)
               1 Group MW Limit Violation (St Albans)
               1 Group MW Limit Violation (Bristol)
               3 Group MVAr Limit Violations (Scotland)
               4 Group MVAr Limit Violations (Leeds)
               1 Group MVAr Limit Violation (Birmingham)

Busbar SUND4   1 Group pole-slipped (Leeds)                Transient Instability
               3 Line Overload Violations (Scotland)
               11 Line Overload Violations (Leeds)
               3 Line Overload Violations (Birmingham)
               1 Line Overload Violation (St Albans)
               16 Voltage Violations (Scotland)
               32 Voltage Violations (Leeds)
               12 Voltage Violations (Birmingham)
               20 Voltage Violations (St Albans)
               17 Voltage Violations (Bristol)
               1 System Frequency Violation
               2 Group MW Limit Violations (Scotland)
               10 Group MW Limit Violations (Leeds)
               3 Group MW Limit Violations (Birmingham)
               4 Group MVAr Limit Violations (Leeds)
               1 Group MVAr Limit Violation (Birmingham)
```

Contingency	Limit Violations/Alarms	System Stability
Line COCK2-STEW2J:L1	2 Groups pole-slipped (Scotland)	Transient Instability
Line STEW2J-ECCL2Q:L1	3 Line Overload Violations (Scotland)	
(Local End Tripped)	5 Line Overload Violations (Leeds)	
	2 Line Overload Violations (Birmingham)	
	15 Voltage Violations (Scotland)	
	27 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	
	6 Group MW Limit Violations (Leeds)	
	3 Group MW Limit Violations (Birmingham)	
	2 Group MVAr Limit Violations (Scotland)	
Busbar WBUR4	1 Group pole-slipped (Leeds)	Transient Instability
	4 Line Overload Violations (Scotland)	
	11 Line Overload Violations (Leeds)	
	3 Line Overload Violations (Birmingham)	
	1 Line Overload Violation (St Albans)	
	17 Voltage Violations (Scotland)	
	33 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	
	1 System Frequency Violation	
	2 Group MW Limit Violations (Scotland)	
	10 Group MW Limit Violations (Leeds)	
	3 Group MW Limit Violations (Birmingham)	
	6 Group MVAr Limit Violations (Leeds)	
	2 Group MVAr Limit Violations (Birmingham)	
	1 Group MVAr Limit Violation (St Albans)	
	1 Group MVAr Limit Violation (Bristol)	
Group RATCLIFFE	1 Group pole-slipped (Leeds)	Transient Instability
	3 Line Overload Violations (Scotland)	
	17 Line Overload Violations (Leeds)	
	3 Line Overload Violations (Birmingham)	
	17 Voltage Violations (Scotland)	
	33 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	
	1 System Frequency Violation	
	1 Group MW Limit Violation (Scotland)	
	9 Group MW Limit Violations (Leeds)	
	2 Group MW Limit Violations (Birmingham)	
	1 Group MVAr Limit Violation (Scotland)	
	4 Group MVAr Limit Violations (Leeds)	
	1 Group MVAr Limit Violation (Birmingham)	
Busbar MELK4	1 Group pole-slipped (Leeds)	Transient Instability
	3 Line Overload Violations (Scotland)	
	14 Line Overload Violations (Leeds)	
	3 Line Overload Violations (Birmingham)	
	1 Line Overload Violation (St Albans)	
	16 Voltage Violations (Scotland)	

Contingency	Limit Violations/Alarms	System Stability
	33 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	
	1 System Frequency Violation	
	2 Group MW Limit Violations (Scotland)	
	9 Group MW Limit Violations (Leeds)	
	3 Group MW Limit Violations (Birmingham)	
	5 Group MVAr Limit Violations (Leeds)	
Line BRLE4-WWEY2K:L1	1 Group pole-slipped (Leeds)	Transient Instability
(Local End Tripped)	3 Line Overload Violations (Scotland)	
	12 Line Overload Violations (Leeds)	
	3 Line Overload Violations (Birmingham)	
	3 Line Overload Violations (St Albans)	
	17 Voltage Violations (Scotland)	
	33 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	
	1 System Frequency Violation	
	2 Group MW Limit Violations (Scotland)	
	10 Group MW Limit Violations (Leeds)	
	3 Group MW Limit Violations (Birmingham)	
	5 Group MVAr Limit Violations (Leeds)	
	1 Group MVAr Limit Violation (Birmingham)	
Busbar EGGB4J	1 Group pole-slipped (Leeds)	Transient Instability
	3 Line Overload Violations (Scotland)	
	14 Line Overload Violations (Leeds)	
	3 Line Overload Violations (Birmingham)	
	1 Line Overload Violation (St Albans)	
	17 Voltage Violations (Scotland)	
	32 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	
	1 System Frequency Violation	
	2 Group MW Limit Violations (Scotland)	
	9 Group MW Limit Violations (Leeds)	
	3 Group MW Limit Violations (Birmingham)	
	1 Group MW Limit Violation (St Albans)	
	1 Group MW Limit Violation (Bristol)	
	6 Group MVAr Limit Violations (Leeds)	
	3 Group MVAr Limit Violations (Birmingham)	
Line DEES4-PENT4:L1	1 Group pole-slipped (Scotland)	Transient Instability
Line DEES4-PENT4:L2	1 Line Overload Violation (Scotland)	
(Remote End Tripped)	6 Line Overload Violations (Leeds)	
	2 Line Overload Violations (Birmingham)	
	14 Voltage Violations (Scotland)	
	26 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	20 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	

Contingency	Limit Violations/Alarms	System Stability
	1 System Frequency Violation	
	5 Group MW Limit Violations (Leeds)	
	2 Group MW Limit Violations (Birmingham)	
	2 Group MVAr Limit Violations (Leeds)	
	3 Group MVAr Limit Violations (Birmingham)	
Busbar DRAK4	1 Group pole-slipped (Leeds)	Transient Instability
	3 Line Overload Violations (Scotland)	
	16 Line Overload Violations (Leeds)	
	4 Line Overload Violations (Birmingham)	
	17 Voltage Violations (Scotland)	
	28 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	19 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	
	1 System Frequency Violation	
	2 Group MW Limit Violations (Scotland)	
	10 Group MW Limit Violations (Leeds)	
	3 Group MW Limit Violations (Birmingham)	
	5 Group MVAr Limit Violations (Leeds)	
	1 Group MVAr Limit Violation (St Albans)	
	1 Group MVAr Limit Violation (Bristol)	
Line NORT4R-HAWP2:L1	1 Group pole-slipped (Scotland)	Transient Instability
Line NORT4R-OSBA4Q:L1	1 Busbar islanded (Leeds)	
(Remote End Tripped)	3 Line Overload Violations (Scotland)	
	11 Line Overload Violations (Leeds)	
	2 Line Overload Violations (Birmingham)	
	17 Voltage Violations (Scotland)	
	31 Voltage Violations (Leeds)	
	8 Voltage Violations (Birmingham)	
	13 Voltage Violations (St Albans)	
	11 Voltage Violations (Bristol)	
	9 Group MW Limit Violations (Leeds)	
	2 Group MW Limit Violations (Birmingham)	
	3 Group MVAr Limit Violations (Scotland)	
	4 Group MVAr Limit Violations (Leeds)	
	2 Group MVAr Limit Violations (Birmingham)	
Busbar KINC2	1 Group pole-slipped (Leeds)	Transient Instability
	2 Line Overload Violations (Scotland)	
	14 Line Overload Violations (Leeds)	
	3 Line Overload Violations (Birmingham)	
	1 Line Overload Violation (St Albans)	
	17 Voltage Violations (Scotland)	
	33 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	20 Voltage Violations (St Albans)	
	14 Voltage Violations (Bristol)	
	1 System Frequency Violation	
	1 Group MW Limit Violation (Scotland)	
	7 Group MW Limit Violations (Leeds)	
	3 Group MW Limit Violations (Birmingham)	
	2 Group MVAr Limit Violations (Scotland)	
	3 Group MVAr Limit Violations (Leeds)	

Contingency	Limit Violations/Alarms	System Stability
Line CRUA2Q-WIYH2:L1 (Local End Tripped)	1 Group pole-slipped (Scotland) 1 Busbar islanded (Scotland) 2 Line Overload Violations (Scotland) 4 Line Overload Violations (Leeds) 2 Line Overload Violations (Birmingham) 16 Voltage Violations (Scotland) 21 Voltage Violations (Leeds) 9 Voltage Violations (Birmingham) 21 Voltage Violations (St Albans) 14 Voltage Violations (Bristol) 2 Group MW Limit Violations (Leeds) 2 Group MW Limit Violations (Birmingham)	Transient Instability
Group WYLFA	5 Groups with undamped oscillations (Scotland) 5 Groups with undamped oscillations (Leeds) 3 Groups with undamped oscillations (Birmingham) 1 Group with undamped oscillations (St Albans) 1 Group with undamped oscillations (Bristol) 2 Line Overload Violations (Scotland) 4 Line Overload Violations (Leeds) 2 Line Overload Violations (Birmingham) 11 Voltage Violations (Scotland) 33 Voltage Violations (Leeds) 12 Voltage Violations (Birmingham) 21 Voltage Violations (St Albans) 17 Voltage Violations (Bristol) 1 Group MW Limit Violation (Leeds)	Dynamic Instability
Group HINKLEY	5 Groups with undamped oscillations (Scotland) 4 Groups with undamped oscillations (Leeds) 2 Groups with undamped oscillations (Birmingham) 1 Group with undamped oscillations (St Albans) 2 Line Overload Violations (Scotland) 4 Line Overload Violations (Leeds) 2 Line Overload Violations (Birmingham) 11 Voltage Violations (Scotland) 33 Voltage Violations (Leeds) 12 Voltage Violations (Birmingham) 21 Voltage Violations (St Albans) 17 Voltage Violations (Bristol) 1 Group MW Limit Violation (Leeds) 3 Group MW Limit Violations (Birmingham)	Dynamic Instability
Load HUER4	5 Groups with undamped oscillations (Scotland) 2 Groups with undamped oscillations (Leeds) 2 Line Overload Violations (Scotland) 4 Line Overload Violations (Leeds) 2 Line Overload Violations (Birmingham) 13 Voltage Violations (Scotland) 32 Voltage Violations (Leeds) 12 Voltage Violations (Birmingham) 21 Voltage Violations (St Albans) 17 Voltage Violations (Bristol)	Dynamic Instability

Contingency	Limit Violations/Alarms	System Stability
Line FIDF2J-HEYS4:L1	4 Groups with undamped oscillations (Scotland)	Dynamic Instability
Line KIBY2-HEYS4:L1	2 Groups with undamped oscillations (Leeds)	
(Remote End Tripped)	2 Line Overload Violations (Scotland)	
	8 Line Overload Violations (Leeds)	
	2 Line Overload Violations (Birmingham)	
	14 Voltage Violations (Scotland)	
	33 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	
	6 Group MW Limit Violations (Leeds)	
	1 Group MW Limit Violation (Birmingham)	
	2 Group MVAr Limit Violations (Leeds)	
Line EGGB4J-PEWO4:L1	2 Groups with undamped oscillations (Scotland)	Dynamic Instability
(Remote End Tripped)	2 Line Overload Violations (Scotland)	
	6 Line Overload Violations (Leeds)	
	2 Line Overload Violations (Birmingham)	
	11 Voltage Violations (Scotland)	
	33 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	
	7 Group MW Limit Violations (Leeds)	
	2 Group MW Limit Violations (Birmingham)	
	5 Group MVAr Limit Violations (Leeds)	
	3 Group MVAr Limit Violations (Birmingham)	
Line IWDQ4-TAUW4Q:L1	2 Groups with undamped oscillations (Scotland)	Dynamic Instability
(Remote End Tripped)	1 Group with undamped oscillations (Leeds)	
	2 Line Overload Violations (Scotland)	
	5 Line Overload Violations (Leeds)	
	2 Line Overload Violations (Birmingham)	
	14 Voltage Violations (Scotland)	
	32 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	
	3 Group MW Limit Violations (Leeds)	
	1 Group MW Limit Violation (Birmingham)	
Load WALH4	2 Line Overload Violations (Scotland)	
	3 Line Overload Violations (Leeds)	
	2 Line Overload Violations (Birmingham)	
	8 Voltage Violations (Scotland)	
	18 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	20 Voltage Violations (St Albans)	
	13 Voltage Violations (Bristol)	
Group DUNGENESS	2 Line Overload Violations (Scotland)	
	3 Line Overload Violations (Leeds)	
	2 Line Overload Violations (Birmingham)	
	11 Voltage Violations (Scotland)	
	33 Voltage Violations (Leeds)	

Contingency	Limit Violations/Alarms	System Stability
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	
	2 Group MW Limit Violations (Leeds)	
	3 Group MW Limit Violations (Birmingham)	
Load IRON4	2 Line Overload Violations (Scotland)	
	3 Line Overload Violations (Leeds)	
	2 Line Overload Violations (Birmingham)	
	6 Voltage Violations (Scotland)	
	15 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	20 Voltage Violations (St Albans)	
	13 Voltage Violations (Bristol)	
Load DRAX4J	2 Line Overload Violations (Scotland)	
	3 Line Overload Violations (Leeds)	
	2 Line Overload Violations (Birmingham)	
	7 Voltage Violations (Scotland)	
	16 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	20 Voltage Violations (St Albans)	
	14 Voltage Violations (Bristol)	
Load FIDF2J	2 Line Overload Violations (Scotland)	
	3 Line Overload Violations (Leeds)	
	2 Line Overload Violations (Birmingham)	
	10 Voltage Violations (Scotland)	
	26 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	
Load PELH4	2 Line Overload Violations (Scotland)	
	3 Line Overload Violations (Leeds)	
	1 Line Overload Violation (Birmingham)	
	6 Voltage Violations (Scotland)	
	14 Voltage Violations (Leeds)	
	10 Voltage Violations (Birmingham)	
	14 Voltage Violations (St Albans)	
	13 Voltage Violations (Bristol)	
Group LONGANNET	2 Line Overload Violations (Scotland)	
	3 Line Overload Violations (Leeds)	
	2 Line Overload Violations (Birmingham)	
	8 Voltage Violations (Scotland)	
	13 Voltage Violations (Leeds)	
	12 Voltage Violations (Birmingham)	
	21 Voltage Violations (St Albans)	
	17 Voltage Violations (Bristol)	
	1 System Frequency Violation	
	1 Group MW Limit Violation (Scotland)	
	5 Group MW Limit Violations (Leeds)	
	2 Group MW Limit Violations (Birmingham)	
	3 Group MVAr Limit Violations (Scotland)	

C.3 Full Alarm List Format

C.3.1 Top Transiently Unstable Contingency

```
        Fuzzy Logic Contingency Ranking and Alarm Processing Summary File

            Sumrank :-   Screening Interval              1.00   secs
                         Fault Duration                  0.08   secs
                         Short Term Dynamics            10.00   secs
                         Longer Term Dynamics           60.00   secs

                         No.  of Line Contingencies        8
                         No.  of Busbar Contingencies      6
                         No.  of Load Contingencies        6
                         No.  of Group Contingencies       6

                         Total No.  of Contingencies      26
                              :                           :

 Contingency Listing System Security Assessment Cycle completed in 9:49 mins

Contingency    Limit Violations/Alarms                    System Stability

Group DRAX.B   Line CLYM2-STHA2:L1 - Overload 110.8%      Transient Instability
               Line COCK2-KINC2:L1 - Overload 116.6%
               Line CREB4-NORT2:L1 - Overload 99.8%
               Line DEES4-FIDF2J:L1 - Overload 93.3%
               Line DRAX4J-KEAD4:L1 - Overload 120.6%
               Line FERR2J-EGGB4J:L1 - Overload 92.5%
               Line HARK2-STHA2:L1 - Overload 163.6%
               Line WBUR4-KEAD4:L1 - Overload 112.5%
               Line WBUR4-WALP4:L1 - Overload 85.9%
               Busbar ABTH2J - Voltage 0.91 pu
               Busbar BLYT2J - Voltage 0.93 pu
               Busbar BRFO4 - Voltage 0.92 pu
               Busbar BRLE4 - Voltage 0.93 pu
               Busbar CANT4 - Voltage 0.95 pu
               Busbar CAPE2J - Voltage 0.95 pu
               Busbar CELL4 - Voltage 0.94 pu
               Busbar CILF4 - Voltage 0.92 pu
               Busbar CLYM2 - Voltage 0.94 pu
               Busbar COCK2 - Voltage 0.93 pu
               Busbar COTT4 - Voltage 0.94 pu
               Busbar COWL4 - Voltage 0.92 pu
               Busbar CREB4 - Voltage 0.94 pu
               Busbar CRUA2Q - Voltage 0.94 pu
               Busbar DAIN4 - Voltage 0.95 pu
               Busbar DEES4 - Voltage 0.95 pu
               Busbar DIDC4 - Voltage 0.92 pu
               Busbar DINO4 - Voltage 0.94 pu
               Busbar DRAK4 - Voltage 0.94 pu
               Busbar DRAX4J - Voltage 0.93 pu
               Busbar DUNG4 - Voltage 0.95 pu
               Busbar ECCL2Q - Voltage 0.92 pu
```

Contingency	Limit Violations/Alarms	System Stability
	Busbar ECLA4 - Voltage 0.91 pu	
	Busbar EGGB4J - Voltage 0.94 pu	
	Busbar ELST2J - Voltage 0.92 pu	
	Busbar EXET4 - Voltage 0.95 pu	
	Busbar FECK4 - Voltage 0.94 pu	
	Busbar FERR2J - Voltage 0.95 pu	
	Busbar FFES2 - Voltage 0.95 pu	
	Busbar FIDF2J - Voltage 0.95 pu	
	Busbar FOYE2 - Voltage 0.95 pu	
	Busbar GALA1 - Voltage 0.89 pu	
	Busbar GRAI4 - Voltage 0.95 pu	
	Busbar HAMH4 - Voltage 0.94 pu	
	Busbar HARK2 - Voltage 0.90 pu	
	Busbar HATL2 - Voltage 0.94 pu	
	Busbar HAWP2 - Voltage 0.94 pu	
	Busbar HEYS4 - Voltage 0.94 pu	
	Busbar HIGM4 - Voltage 0.94 pu	
	Busbar HINP4 - Voltage 0.95 pu	
	Busbar HUER4 - Voltage 0.95 pu	
	Busbar INDQ4 - Voltage 0.94 pu	
	Busbar IRON4 - Voltage 0.95 pu	
	Busbar IVER2J - Voltage 0.92 pu	
	Busbar KEAD4 - Voltage 0.94 pu	
	Busbar KEAR4Q - Voltage 0.95 pu	
	Busbar KEMS4J - Voltage 0.95 pu	
	Busbar KIBY2 - Voltage 0.95 pu	
	Busbar KILS2 - Voltage 0.94 pu	
	Busbar KING2 - Voltage 0.93 pu	
	Busbar KING4 - Voltage 0.95 pu	
	Busbar KINT2 - Voltage 0.95 pu	
	Busbar LEGA4 - Voltage 0.94 pu	
	Busbar LITT4 - Voltage 0.94 pu	
	Busbar LOAN2 - Voltage 0.94 pu	
	Busbar LOVE4 - Voltage 0.94 pu	
	Busbar MAYT1T - Voltage 0.92 pu	
	Busbar MELK4 - Voltage 0.93 pu	
	Busbar NEIL2 - Voltage 0.95 pu	
	Busbar NFLW4R - Voltage 0.95 pu	
	Busbar NFLW4S - Voltage 0.94 pu	
	Busbar NORT2 - Voltage 0.93 pu	
	Busbar NORT4R - Voltage 0.92 pu	
	Busbar OSBA4Q - Voltage 0.93 pu	
	Busbar PEHE2 - Voltage 0.94 pu	
	Busbar PELH4 - Voltage 0.91 pu	
	Busbar PEMB4 - Voltage 0.93 pu	
	Busbar PENN2 - Voltage 0.94 pu	
	Busbar PENT4 - Voltage 0.94 pu	
	Busbar PEWO4 - Voltage 0.94 pu	
	Busbar RATS4J - Voltage 0.94 pu	
	Busbar RUGE4 - Voltage 0.95 pu	
	Busbar STAL4Q - Voltage 0.95 pu	
	Busbar STEW2J - Voltage 0.93 pu	
	Busbar STHA2 - Voltage 0.93 pu	
	Busbar STSB4 - Voltage 0.94 pu	
	Busbar SUND4 - Voltage 0.91 pu	

Contingency	Limit Violations/Alarms	System Stability
	Busbar SWAN4 - Voltage 0.92 pu	
	Busbar TAUN4Q - Voltage 0.95 pu	
	Busbar TAUN4R - Voltage 0.95 pu	
	Busbar THOM2J - Voltage 0.94 pu	
	Busbar THOM4 - Voltage 0.95 pu	
	Busbar TILB4R - Voltage 0.94 pu	
	Busbar TRAW2 - Voltage 0.95 pu	
	Busbar TRAW4 - Voltage 0.94 pu	
	Busbar WALH4 - Voltage 0.93 pu	
	Busbar WALP4 - Voltage 0.91 pu	
	Busbar WALX4Q - Voltage 0.91 pu	
	Busbar WALX4R - Voltage 0.91 pu	
	Busbar WBOL2 - Voltage 0.93 pu	
	Busbar WBUR4 - Voltage 0.93 pu	
	Busbar WHSO2 - Voltage 0.91 pu	
	Busbar WHSO4Q - Voltage 0.92 pu	
	Busbar WILL4 - Voltage 0.94 pu	
	Busbar WISD2 - Voltage 0.93 pu	
	Busbar WISH2 - Voltage 0.95 pu	
	Busbar WIYH2 - Voltage 0.95 pu	
	Busbar WTHU2J - Voltage 0.92 pu	
	Busbar WWEY2K - Voltage 0.92 pu	
	Busbar WYLF4 - Voltage 0.94 pu	
	Group COTTAM - on MW Limits	
	Group COTTAM - on MVAr Limits	
	Group CRUACHAN - on MVAr Limits	
	Group DINORWIG - on MW Limits	
	Group EGGBORO. - on MW Limits	
	Group EGGBORO. - on MVAr Limits	
	Group FERRYBR. - on MW Limits	
	Group FERRYBR. - on MVAr Limits	
	Group FIDDLERS - on MW Limits	
	Group HEYSHAM - on MW Limits	
	Group LONGANNET - on MVAr Limits	
	Group RATCLIFFE - on MW Limits	
	Group RUGELEY - on MW Limits	
	Group CRUACHAN (pole-slipped)	
	Line BLYT2J-WBOL2:L1 - Overload 107.6%	
	Line COCK2-ECCL2Q:L1 - Overload 88.2%	
	Line COCK2-STEW2J:L1 - Overload 93.3%	
	Line DINO4-PENT4:L1 - Overload 88.9%	
	Line DINO4-PENT4:L2 - Overload 88.2%	
	Line DRAX4J-EGGB4J:L1 - Overload 86.5%	
	Line FIDF2J-KIBY2:L1 - Overload 115.7%	
	Line HATL2-HAWP2:L1 - Overload 121.6%	
	Line HATL2-NORT2:L1 - Overload 115.5%	
	Line HATL2-WBOL2:L1 - Overload 85.3%	
	Line HEYS4-HARK2:L1 - Overload 107.6%	
	Line HEYS4-HARK2:L2 - Overload 107.6%	
	Line HUER4-KILS2:L1 - Overload 92.1%	
	Line HUER4-NEIL2:L1 - Overload 116.8%	
	Line NEIL2-STHA2:L1 - Overload 89.1%	
	Line NORT2-STEW2J:L1 - Overload 106.8%	
	Line NORT4R-HAWP2:L1 - Overload 114.6%	
	Line PEWO4-HARK2:L1 - Overload 114.7%	

Contingency	Limit Violations/Alarms	System Stability
	Line STEW2J-ECCL2Q:L1 - Overload 94.2%	
	Group DINORWIG - on MVAr Limits	
	Group DUNGENESS - on MW Limits	
	Group FFESTIN. - on MVAr Limits	
	Group HARTLEPL. - on MW Limits	
	Group HINKLEY - on MW Limits	
	Group HUNTERSTN - on MVAr Limits	
	Group TRAWS. - on MW Limits	
	Group WYLFA - on MW Limits	

C.3.2 Top Dynamically Unstable Contingency

Fuzzy Logic Contingency Ranking and Alarm Processing Summary File

Sumrank :-	Screening Interval	1.00	secs
	Fault Duration	0.08	secs
	Short Term Dynamics	10.00	secs
	Longer Term Dynamics	60.00	secs
	No. of Line Contingencies	8	
	No. of Busbar Contingencies	6	
	No. of Load Contingencies	6	
	No. of Group Contingencies	6	
	Total No. of Contingencies	26	

Contingency Listing System Security Assessment Cycle completed in 9:49 mins

Contingency	Limit Violations/Alarms	System Stability
Group WYLFA	Line CLYM2-STHA2:L1 - Overload 110.8%	Dynamic Instability
	Line COCK2-KINC2:L1 - Overload 105.1%	
	Line DEES4-FIDF2J:L1 - Overload 93.3%	
	Line DRAX4J-KEAD4:L1 - Overload 120.6%	
	Line HARK2-STHA2:L1 - Overload 163.6%	
	Line KIBY2-HEYS4:L1 - Overload 85.5%	
	Line WBUR4-KEAD4:L1 - Overload 112.5%	
	Line WBUR4-WALP4:L1 - Overload 85.9%	
	Busbar ABTH2J - Voltage 0.91 pu	
	Busbar BLYT2J - Voltage 0.93 pu	
	Busbar BRFO4 - Voltage 0.92 pu	
	Busbar BRLE4 - Voltage 0.93 pu	
	Busbar CANT4 - Voltage 0.95 pu	
	Busbar CAPE2J - Voltage 0.95 pu	
	Busbar CELL4 - Voltage 0.94 pu	
	Busbar CILF4 - Voltage 0.92 pu	
	Busbar CLYM2 - Voltage 0.95 pu	
	Busbar COCK2 - Voltage 0.93 pu	
	Busbar COTT4 - Voltage 0.94 pu	
	Busbar COWL4 - Voltage 0.92 pu	
	Busbar CREB4 - Voltage 0.94 pu	
	Busbar DAIN4 - Voltage 0.95 pu	
	Busbar DEES4 - Voltage 0.95 pu	
	Busbar DIDC4 - Voltage 0.92 pu	
	Busbar DINO4 - Voltage 0.95 pu	
	Busbar DRAK4 - Voltage 0.94 pu	
	Busbar DRAX4J - Voltage 0.95 pu	
	Busbar DUNG4 - Voltage 0.95 pu	
	Busbar ECCL2Q - Voltage 0.92 pu	
	Busbar ECLA4 - Voltage 0.91 pu	
	Busbar EGGB4J - Voltage 0.95 pu	
	Busbar ELST2J - Voltage 0.92 pu	
	Busbar EXET4 - Voltage 0.95 pu	
	Busbar FECK4 - Voltage 0.94 pu	

Contingency	Limit Violations/Alarms	System Stability
	Busbar FERR2J - Voltage 0.95 pu	
	Busbar FFES2 - Voltage 0.95 pu	
	Busbar FIDF2J - Voltage 0.95 pu	
	Busbar GALA1 - Voltage 0.89 pu	
	Busbar GRAI4 - Voltage 0.95 pu	
	Busbar HAMH4 - Voltage 0.94 pu	
	Busbar HARK2 - Voltage 0.90 pu	
	Busbar HATL2 - Voltage 0.94 pu	
	Busbar HAWP2 - Voltage 0.94 pu	
	Busbar HEYS4 - Voltage 0.94 pu	
	Busbar HIGM4 - Voltage 0.94 pu	
	Busbar HIMP4 - Voltage 0.95 pu	
	Busbar INDQ4 - Voltage 0.94 pu	
	Busbar IRON4 - Voltage 0.95 pu	
	Busbar IVER2J - Voltage 0.92 pu	
	Busbar KEAD4 - Voltage 0.94 pu	
	Busbar KEAR4Q - Voltage 0.95 pu	
	Busbar KEMS4J - Voltage 0.95 pu	
	Busbar KIBY2 - Voltage 0.95 pu	
	Busbar KILS2 - Voltage 0.95 pu	
	Busbar KING2 - Voltage 0.95 pu	
	Busbar KING4 - Voltage 0.95 pu	
	Busbar LEGA4 - Voltage 0.95 pu	
	Busbar LITT4 - Voltage 0.94 pu	
	Busbar LOAN2 - Voltage 0.95 pu	
	Busbar LOVE4 - Voltage 0.94 pu	
	Busbar MAYT1T - Voltage 0.92 pu	
	Busbar MELK4 - Voltage 0.93 pu	
	Busbar NEIL2 - Voltage 0.95 pu	
	Busbar NFLW4R - Voltage 0.95 pu	
	Busbar NFLW4S - Voltage 0.94 pu	
	Busbar NORT2 - Voltage 0.93 pu	
	Busbar NORT4R - Voltage 0.95 pu	
	Busbar OSBA4Q - Voltage 0.95 pu	
	Busbar PELH4 - Voltage 0.91 pu	
	Busbar PEMB4 - Voltage 0.93 pu	
	Busbar PENN2 - Voltage 0.94 pu	
	Busbar PENT4 - Voltage 0.95 pu	
	Busbar PEWO4 - Voltage 0.94 pu	
	Busbar RATS4J - Voltage 0.94 pu	
	Busbar RUGE4 - Voltage 0.95 pu	
	Busbar STAL4Q - Voltage 0.95 pu	
	Busbar STEW2J - Voltage 0.93 pu	
	Busbar STHA2 - Voltage 0.95 pu	
	Busbar STSB4 - Voltage 0.95 pu	
	Busbar SUND4 - Voltage 0.91 pu	
	Busbar SWAN4 - Voltage 0.92 pu	
	Busbar TAUN4Q - Voltage 0.95 pu	
	Busbar TAUN4R - Voltage 0.95 pu	
	Busbar THOM2J - Voltage 0.95 pu	
	Busbar THOM4 - Voltage 0.95 pu	
	Busbar TILB4R - Voltage 0.94 pu	
	Busbar TRAW2 - Voltage 0.95 pu	
	Busbar TRAW4 - Voltage 0.95 pu	
	Busbar WALH4 - Voltage 0.93 pu	

Contingency	Limit Violations/Alarms	System Stability
	Busbar WALP4 - Voltage 0.91 pu	
	Busbar WALX4Q - Voltage 0.91 pu	
	Busbar WALX4R - Voltage 0.91 pu	
	Busbar WBOL2 - Voltage 0.93 pu	
	Busbar WBUR4 - Voltage 0.93 pu	
	Busbar WHSO2 - Voltage 0.91 pu	
	Busbar WHSO4Q - Voltage 0.92 pu	
	Busbar WILL4 - Voltage 0.94 pu	
	Busbar WISD2 - Voltage 0.93 pu	
	Busbar WISH2 - Voltage 0.95 pu	
	Busbar WTHU2J - Voltage 0.92 pu	
	Busbar WWEY2K - Voltage 0.92 pu	
	Busbar WYLF4 - Voltage 0.95 pu	
	Group COTTAM (undamped oscillations)	
	Group CRUACHAN (undamped oscillations)	
	Group DINORWIG (undamped oscillations)	
	Group DUNGENESS (undamped oscillations)	
	Group EGGBORO. (undamped oscillations)	
	Group FFESTIN. (undamped oscillations)	
	Group FIDDLERS (undamped oscillations)	
	Group FOYERS (undamped oscillations)	
	Group HINKLEY (undamped oscillations)	
	Group HUNTERSTN (undamped oscillations)	
	Group LONGANNET (undamped oscillations)	
	Group PETERHEAD (undamped oscillations)	
	Group RATCLIFFE (undamped oscillations)	
	Group RUGELEY (undamped oscillations)	
	Group TRAWS. (undamped oscillations)	
	Group FIDDLERS (parameters ramping)	
	Group DINORWIG - on MW Limits	

C.3.3 Top Stable Contingency

```
      Fuzzy Logic Contingency Ranking and Alarm Processing Summary File


          Sumrank :-  Screening Interval              1.00   secs
                      Fault Duration                  0.08   secs
                      Short Term Dynamics            10.00   secs
                      Longer Term Dynamics           60.00   secs

                      No.  of Line Contingencies        8
                      No.  of Busbar Contingencies      6
                      No.  of Load Contingencies        6
                      No.  of Group Contingencies       6

                      Total No.  of Contingencies      26


Contingency Listing System Security Assessment Cycle completed in 9:49 mins

   Contingency  Limit Violations/Alarms                    System Stability

   Load WALH4   Line CLYM2-STHA2:L1 - Overload 111.0%
                Line COCK2-KINC2:L1 - Overload 104.2%
                Line DEES4-FIDF2J:L1 - Overload 93.6%
                Line DRAX4J-KEAD4:L1 - Overload 121.3%
                Line HARK2-STHA2:L1 - Overload 163.9%
                Line WBUR4-KEAD4:L1 - Overload 113.1%
                Line WBUR4-WALP4:L1 - Overload 86.4%
                Busbar ABTH2J - Voltage 0.92 pu
                Busbar BLYT2J - Voltage 0.93 pu
                Busbar BRFO4 - Voltage 0.92 pu
                Busbar BRLE4 - Voltage 0.93 pu
                Busbar CANT4 - Voltage 0.95 pu
                Busbar CELL4 - Voltage 0.95 pu
                Busbar CILF4 - Voltage 0.93 pu
                Busbar COCK2 - Voltage 0.93 pu
                Busbar COTT4 - Voltage 0.94 pu
                Busbar COWL4 - Voltage 0.93 pu
                Busbar CREB4 - Voltage 0.94 pu
                Busbar DAIN4 - Voltage 0.95 pu
                Busbar DIDC4 - Voltage 0.93 pu
                Busbar DRAK4 - Voltage 0.95 pu
                Busbar ECCL2Q - Voltage 0.92 pu
                Busbar ECLA4 - Voltage 0.92 pu
```

Contingency	Limit Violations/Alarms	System Stability
	Busbar ELST2J - Voltage 0.92 pu	
	Busbar FECK4 - Voltage 0.94 pu	
	Busbar GALA1 - Voltage 0.89 pu	
	Busbar GRAI4 - Voltage 0.95 pu	
	Busbar HAMH4 - Voltage 0.94 pu	
	Busbar HARK2 - Voltage 0.90 pu	
	Busbar HATL2 - Voltage 0.94 pu	
	Busbar HAWP2 - Voltage 0.94 pu	
	Busbar HEYS4 - Voltage 0.94 pu	
	Busbar HIGM4 - Voltage 0.94 pu	
	Busbar INDQ4 - Voltage 0.94 pu	
	Busbar IRON4 - Voltage 0.95 pu	
	Busbar IVER2J - Voltage 0.92 pu	
	Busbar KEAD4 - Voltage 0.94 pu	
	Busbar KEAR4Q - Voltage 0.95 pu	
	Busbar KEMS4J - Voltage 0.95 pu	
	Busbar KINC2 - Voltage 0.95 pu	
	Busbar KINO4 - Voltage 0.95 pu	
	Busbar LITT4 - Voltage 0.94 pu	
	Busbar LOVE4 - Voltage 0.94 pu	
	Busbar MAYT1T - Voltage 0.92 pu	
	Busbar MELK4 - Voltage 0.94 pu	
	Busbar NFLW4S - Voltage 0.94 pu	
	Busbar NORT2 - Voltage 0.93 pu	
	Busbar NORT4R - Voltage 0.95 pu	
	Busbar PELH4 - Voltage 0.91 pu	
	Busbar PEMB4 - Voltage 0.93 pu	
	Busbar PENN2 - Voltage 0.95 pu	
	Busbar PEWO4 - Voltage 0.94 pu	
	Busbar RATS4J - Voltage 0.95 pu	
	Busbar STAL4Q - Voltage 0.95 pu	
	Busbar STEW2J - Voltage 0.93 pu	
	Busbar STHA2 - Voltage 0.95 pu	
	Busbar SUND4 - Voltage 0.91 pu	
	Busbar SWAN4 - Voltage 0.93 pu	
	Busbar THOM2J - Voltage 0.95 pu	
	Busbar THOM4 - Voltage 0.95 pu	
	Busbar TILB4R - Voltage 0.94 pu	
	Busbar WALH4 - Voltage 0.94 pu	
	Busbar WALP4 - Voltage 0.91 pu	
	Busbar WALX4Q - Voltage 0.91 pu	
	Busbar WALX4R - Voltage 0.91 pu	
	Busbar WBOL2 - Voltage 0.93 pu	
	Busbar WBUR4 - Voltage 0.93 pu	

Contingency	Limit Violations/Alarms	System Stability
	Busbar WHSO2 - Voltage 0.91 pu	
	Busbar WHSO4Q - Voltage 0.93 pu	
	Busbar WILL4 - Voltage 0.94 pu	
	Busbar WISD2 - Voltage 0.94 pu	
	Busbar WISH2 - Voltage 0.95 pu	
	Busbar WTHU2J - Voltage 0.92 pu	
	Busbar WWEY2K - Voltage 0.93 pu	
	Busbar CLYM2 - Voltage 0.95 pu	
	Busbar NFLW4R - Voltage 0.95 pu	
	Busbar RUGE4 - Voltage 0.95 pu	
	Busbar STSB4 - Voltage 0.95 pu	

Appendix D

Published Work

1. GROOM, C. G., CHAN, K. W., DUNN, R. W. AND DANIELS, A. R.: 'Fuzzy Logic Techniques Applied to Power System Control', Proc. 29th Universities' Power Engineering Conference, Vol. 2, pp. 832–835, 1994.

FUZZY LOGIC TECHNIQUES APPLIED TO POWER SYSTEM CONTROL

C.G.Groom, K.W.Chan, R.W.Dunn, A.R.Daniels

School of Electronic and Electrical Engineering, University of Bath, Avon, UK

Abstract

This paper describes the use of fuzzy sets in the area of power system security assessment which includes identification of electromechanical modes of operation, contingency screening and evaluation and subsequent alarm processing. The application of this technique as part of a complete real-time dynamic security assessment system written at the University of Bath is discussed and results are presented for an IEEE test network, together with a reduced UK National Grid system. Comparisons will be made between this new method and more traditional numerical approaches, illustrating the improvements that can be made in the operation of complex power systems.

1 INTRODUCTION

Power system security can be defined as the ability of the system to continue normal operation despite the occurrence of any one of a pre-selected list of credible disturbances or "contingencies". This concept has become increasingly of interest to power utilities since networks are being operated ever closer to their stability limits due to cost, efficiency and environmental constraints.

Many techniques have been developed over a number of decades to study system instability, contingency analysis and alarm processing which encompass a wide range of techniques. These are, principally, numerical- or algorithmical-based and artificial intelligence (such as expert systems and pattern recognition) approaches which have been gradually enhanced over a number of years of research. Numerical methods are limited in that they rely heavily on a mathematical model of how the process behaves. Some systems (such as power networks) are not amenable to this type of treatment and hence mathematical theory cannot be successfully applied in all cases. Artificial intelligence techniques, differ since they try to model the skills of the operator and not the process itself.

In this paper, the expert system approach based on *fuzzy set theory* will be discussed and how its application to deal with the analysis of a non-linear system such as a power network will be described.

2 METHODOLOGY

The principle behind fuzzy logic [1, 2, 3, 4] is to represent humanistic knowledge in a form recognisable to both man and machine. An operator may have a theory about what is the best thing to do whilst controlling a process and may express it using rules which contain vague terms such as "small", "slightly", etc ... This can be represented by fuzzy logic using set theory. *Linguistic Variables* are used in place of numerical quantities and are statements which have values described in some natural language, such as the variable *size* may have values *small*, *medium*, *large*, etc ... These values can be further described by the use of *Linguistic Hedges* such as *very*, *not* and *likely*. The linguistic variables can be equated by *Fuzzy Conditional Statements* in the form **"If A Then B Else C"**, which can subsequently be grouped together to form *Fuzzy Algorithms* or an ordered sequence of events containing fuzzy assignment and conditional statements.

The linguistic variable *size* can be represented by Figure 1.

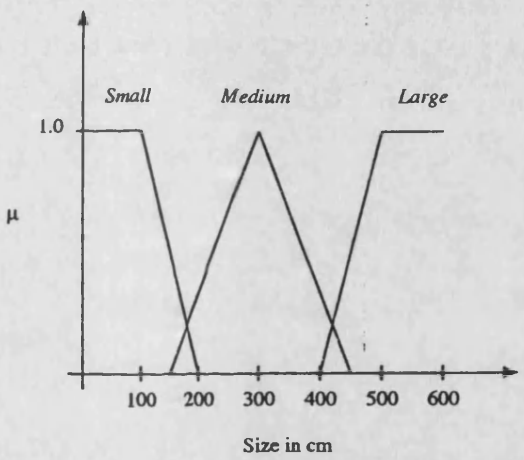


Figure 1: Membership Function (μ) vs Linguistic Variable (*Size*)

Here, there will be a range of sizes which will definitely apply and will have a *grade of membership* μ in the set of 1. Conversely, there will be a range over which the term does not apply, with μ in the set of 0. Unlike more traditional set theory, fuzzy logic dictates that there is a region where the variable does not cover the full scale and will have a μ between 0 and 1.

It is due to this overlap that fuzzy set theory can help in filling the gaps in the knowledge-base and dealing with the imprecision of the operator, since there will be conditions where more than one rule can apply at a given time. It is this effect that can be exploited in security analysis of power systems.

3 APPLICATIONS TO POWER SYSTEM SECURITY

3.1 Contingency Analysis

Security Assessment has become a valuable tool in the analysis of power system operation under fault conditions and

is probably the most time-consuming function in an Energy Management System or EMS. This is because on-line contingency analysis is often performed automatically over typical time intervals of ten to twenty minutes.
For large power systems, hundreds, or in some cases, thousands of contingencies would need to be fully analysed within very short time intervals which imposes a considerable computational burden on EMS computers. Systematic approaches have been developed to automatically select the critical contingencies [5, 6, 7] to reduce the full analysis time and rank them in their ascending order of severity. *Performance indices* (PI) of the form

$$PI = \sum_{i=1}^{N} w_i \left[\frac{X_i}{X_i^{max}} \right]^n \qquad (1)$$

are often used, where X_i is a transmission line power flow or change in busbar voltage magnitude, X_i^{max} is the corresponding thermal rating and maximum permissible voltage change, respectively and, w_i is a non-negative weighting coefficient. The PI is then calculated for all the lines and/or busbars in the system. With a value of the exponent n in Equation 1 equal to two, the performance index can be prone to *masking errors*, where a contingency with many small limit violations can be ranked equally with one with a few large limit violations.
A fuzzy set approach (based on [8]) presented in this paper has been modified and implemented for contingency screening, evaluation and ranking Busbar voltages, transmission line flows and real and reactive power injections during and after a contingency application are classified into one of five fuzzy linguistic variable sets, i.e. very small VS, small S, medium, M, large L and very large VL, which are characterised in triangular form by a sigmoid function as in Figure 2.
To quantify these linguistic variables, a performance index (PI) is used to describe the relative severity of each variable, i.e. a higher PI indicates a greater chance of large limit violations. The membership function μ for each variable is described by the triangle's centre C (the most likely value of the PI for the variable), width W (the degree of uncertainty about the PI) and peak value P (the strength of the variable). By using the sigmoid function in Figure 2, more emphasis has been placed on the variables medium to very large, i.e. the more severe cases, to avoid the masking problem.
If during a contingency, more than one violation from the system falls under a particular linguistic variable description, the membership function of that category is modified by fuzzy set notation. This means that the peak value P increases by multiplying μ by the number of violations that have occurred in that category.
Once all the triangles have been modified at the end of the contingency application, it is necessary to "defuzzify" the membership functions to yield the overall system performance index for that particular contingent quantity. A *centre of gravity* algorithm or (product-sum) by binary search is used for greater accuracy rather than the less computationally demanding max-min method. These indices for each contingent quantity are then summed together to give the total system severity index (SI).

3.2 Instability Detection

Power systems are examples of non-linear systems with a wide range of stability problems where the main areas of interest are,

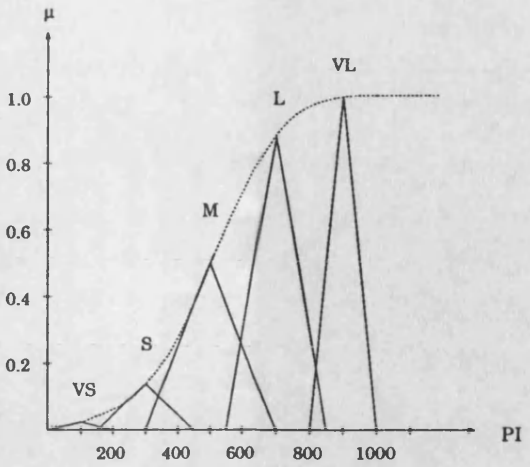


Figure 2: Membership Function (μ) vs Performance Index (PI) using the Sigmoid Function

primarily, the behaviour of synchronous generators during a large system disturbance or contingency. In these stability studies, both short-term as well as the longer-term dynamics of the system should be simulated and analysed.
Conventionally, *transient stability* programs have been used to study the fast synchronising oscillations following a large disturbance, with a typical simulation of one to ten seconds. *Dynamic stability* algorithms ignore these fast machine oscillations and concentrate on the longer-term effects of slow power and voltage swings and frequency deviations resulting from energy imbalances over a simulation time interval of tens of minutes.
Traditionally, both transient and dynamic stability analyses have been carried out by numerical techniques such as the "transient energy function" [9, 10] and eigenvalue evaluation [11, 12] respectively. These can be time-consuming and not totally accurate for large systems. Hence an approach using fuzzy set classification, similar to that for contingency analysis, has been developed using generator machine rotor angle, rotor acceleration and kinetic energy for transient studies and power oscillation and ramping/interaction between neighbouring machine parameters for dynamic instability, which has shown to be accurate and adaptable for any size of power network.

3.3 Alarm Handling

With any security analysis program and considering the size and complexity of a typical modern power system, an operator cannot be expected to process all the information available during fault conditions. It is because of this that alarm processors have been developed [13, 14], which evaluate the importance of each message and help the operator to track the evolution of the power system state during a disturbance by providing a summary of the abnormal conditions. Here again fuzzy sets can help in the decision making of alarm handling and data processing using the methods outlined above.

4 RESULTS

A time domain solution method has been used for this paper based on a real-time simulator, PowSim, of a 10^{th} order

power system model (including synchronous generators and their associated controllers) developed at the University of Bath [15, 16]. A single processor version of this running on an Intel i860-based PC was used to simulate both an IEEE 57 bus [17] test network and a reduced 100 bus NGC system for both fuzzy and traditional approaches of security assessment.

4.1 Procedure

Time simulations using a time step of 40 ms were run for each contingency in a pre-determined database consisting of single or multiple transmission line outages, 3-phase to ground faults on busbars, busbar load losses and generator trips for a screening period of one second. Those cases that produce limit violations (from the alarm processor) were added to a memory stack list for a subsequent analysis, or evaluation period, of ten seconds. If transient instability occurred during the one second time interval, these contingencies were screened out and placed at the top of the final ranking order, since these are naturally the most severe cases. If after the evaluation interval, undamped or, at least, poorly damped power oscillations were still present, the time simulation was extended to determine the system state after a further sixty seconds for dynamic instability detection. Results for each test system are given below for both the fuzzy method and the more traditional numerical approach.

4.2 IEEE 57 Bus System

A database of 312 contingencies was used to test the algorithms for this network. A numerical method using an exponent value $n = 20$ from Equation 1 was used as the "benchmark", since it has been proved that this will remove any masking errors at the expense of computational speed and, hence, result in greater ranking accuracy.

Table 1 shows the security assessment results for this case study. The number of misrankings for the $n = 2$ method compared to that of the benchmark increase with the number of ranked contingencies which can be explained by the masking effect. The fuzzy set approach has, in contrast, very few misrankings, those that were present are not significantly different to those from the benchmark. It should also be noted that this technique has a considerable speed-up advantage over the latter, due to the absence of increased computation.

4.3 Reduced NGC 100 Bus System

The reduced NGC system used comprises of 100 busbars and 20 synchronous generators. This gives a contingency database of 854 entries and again the same benchmark was used for comparison purposes.

The results in Table 2 show two entries for each method, the top is for a "summer night-time loading" condition and, the bottom. for an enhanced operating state with increased transfer from Scotland to England causing dynamic instability for some cases. Again the misrankings are prominent for the $n = 2$ method, with very few errors between the fuzzy and benchmark approaches.

5 CONCLUSIONS

In this paper a fuzzy set approach has been used to address the areas of stability detection, contingency analysis and alarm processing. Although this methodology has been tried in previous research, power system models of the size tested in this study have not been attempted and, in the case of contingency evaluation, a real-time power system simulator approach has not been used before.

The results that have been presented have shown a favourable speed-up in execution time as compared to the more traditional numerical techniques. With the ever-increasing power of modern processors and distributed system architectures, the fuzzy set approach is a practical and adaptable technique for security analysis studies for any size of power system, without the errors and results interpretation often associated with mathematical methods.

References

[1] L.A. Zadeh. "Outline of a New Approach to the Analysis of Complex Systems and Decision Processes". In *IEEE Transactions on Systems, Man and Cybernetics, Vol. 3*, pages 28–44, January 1973.

[2] C.P. Pappis and E.H. Mamdani. "A Fuzzy Logic Controller for a Traffic Junction". In *IEEE Transactions on Systems, Man and Cybernetics, Vol. 7*, pages 707–717, October 1977.

[3] A.N.S. Freeling. "Fuzzy Sets and Decision Analysis". In *IEEE Transactions on Systems, Man and Cybernetics, Vol. 10*, pages 341–354, July 1980.

[4] J. Efstathiou. "Expert Systems, Fuzzy Logic and Rule-Based Controllers". In *Transactions of Inst. MC, Vol. 10*, pages 198–206, July 1988.

[5] G.C. Ejebe and B.F. Wollenberg. "Automatic Contingency Selection". In *IEEE Transactions on Power Apparatus and Systems, Vol. 98*, pages 97–107, January 1979.

[6] S. Vemuri and R.E. Usher. "On-Line Automatic Contingency Selection Algorithms". In *IEEE Transactions on Power Apparatus and Systems, Vol. 102*, pages 346–354, January 1983.

[7] A.O. Ekwue. "A Review of Automatic Contingency Selection Algorithms of On-Line Security Analysis". In *IEE 3rd International Conference on Power System Monitoring and Control*, pages 152–155, 1990.

[8] Y.Y. Hsu and K. Han-Ching. "Fuzzy-Set Based Contingency Ranking". In *IEEE Transactions on Power Systems, Vol. 7*, pages 1189–1195, August 1992.

[9] S. Vemuri and R.E. Usher. "Critical Energy for Direct Transient Stability Assessment of a Multimachine Power System". In *IEEE Transactions on Power Apparatus and Systems, Vol. 103*, pages 2199–2206, August 1984.

[10] CIGRE task force 38.02.09. "Assessment of Practical Fast Transient Stability Methods — State of the Art Report". Technical report, CIGRE, 1992.

[11] B. Ramsay and J.L. Sulley. "Dynamic Stability of Plant in the North of Scotland Hydro-Electric Board Network". In *8th PSCC, Helsinki, Vol. 6*, pages 990–996, August 1984.

[12] D.Y. Wong, G.J. Rogers, B. Poretta, and P. Kundur. "Eigenvalue Analysis of Very Large Power Systems". In *IEEE Transactions on Power Systems, Vol. 3*, pages 472–480, May 1988.

Security Assessment Algorithm	No. of Misrankings		No. of Stability Cases		Solution Time in minutes
	1^{st} Ten	1^{st} Twenty	Transient	Dynamic	
Numerical (n = 2)	2	7	0	0	10.93
Numerical (n = 20)	-	-	0	0	19.06
Fuzzy-Set	1	3	0	0	9.6

Table 1: Results for IEEE 57 Bus Network

Security Assessment Algorithm	No. of Misrankings		No. of Stability Cases		Solution Time in minutes
	1^{st} Ten	1^{st} Twenty	Transient	Dynamic	
Numerical (n = 2)	7	13	22	0	92.68
	8	15	563	9	193.4
Numerical (n = 20)	-	-	22	0	128.26
	-	-	563	9	270.48
Fuzzy-Set	2	3	22	0	72.16
	3	5	563	9	153.35

Table 2: Results for NGC 100 Bus Network

[13] B.F. Wollenberg. "Feasibility Study for an Energy Management System Intelligent Alarm Processor". In *IEEE Transactions on Power Systems, Vol. 1*, pages 241–246, May 1986.

[14] D.S. Kirschen and B.F. Wollenberg. "Intelligent Alarm Processing in Power Systems". In *Proceedings of IEEE, Vol. 80*, pages 663–672, May 1992.

[15] L.A. Dale, A.R. Daniels, and I.A. Erinmez. "The Real-Time Modelling of the Operation of Complex Power Systems". In *Proceedings of 21st Universities' Power Engineering Conference*, pages 181–183, September 1985.

[16] T. Berry, K.W. Chan, Daniels A.R., and Dunn R.W. "Interactive Real-Time Simulation of the Dynamic Behaviour of Large Power Systems". In *Proc of the 4th Annual Conference of Power and Energy Society IEE Japan*, pages 5–10, July 1993.

[17] L.L. Freris and A.M. Sasson. "Investigation of the Load Flow Problem". In *Proceedings of IEE, Vol. 115*, pages 1459–1470, October 1968.

ACKNOWLEDGEMENT

The continual technical and financial support of the NGC is gratefully acknowledged, and, in particular, that of Mr P.H.Buxton for his useful comments which have been very welcome.

ADDRESS

The work described in this paper is on-going and the authors may be contacted at the following address.

Power and Energy Systems Group,
School of Electronic and Electrical Engineering,
University of Bath,
Claverton Down,
Bath,
Avon BA2 7AY.

Email : chris@uk.ac.bath.ee